Bundesamt
für Sicherheit in der
Informationstechnik

Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Anlage

1. Einleitung

Die zunehmende Vernetzung von Rechnern und Rechnerverbünden hat einen Wandel im Kommunikationsverhalten der Behörden und Unternehmen bewirkt. Neben der Suche nach Informationen zur Erleichterung der Aufgabenerledigung wird vor allem das Internet zunehmend als universelles Transportmedium für Daten benutzt. Es gilt deshalb, bei der Nutzung von nicht-vertrauenswürdigen Netzen – ein solches stellt eben das Internet dar – zur Übertragung von schutzwürdigen Daten Sicherungsmaßnahmen wie Verschlüsselung und Authentisierung zu ergreifen. Dies kann beispielsweise mit Hilfe von „Virtual Private Networks“ erfolgen.

Ein Virtual Private Network (VPN) ist ein Netz, das physikalisch innerhalb eines anderen Netzes (meist des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. VPNs können unter anderem mit Hilfe kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten schützen und die Kommunikationspartner sicher authentisieren, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff Virtual Private Network wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden. Beispiele hierfür sind:

- physische Trennung der Daten, z. B. mit dedizierten Leitungen
- logische Trennung der Daten, z. B. mit VLANs (“Virtual Local Area Network”)
- Beide voranstehenden Methoden werden vom Provider umgesetzt und unter dem Begriff „Trusted VPNs“ zusammengefasst, da dem Provider die Sicherheit der Daten anvertraut wird.
- Neben der Umsetzung des VPNs durch Provider kann ein VPN auch durch die Institution erzeugt werden, die das VPN nutzt. Die Absicherung der Daten geschieht in diesem Fall mit Hilfe von kryptographischen Verfahren, weshalb diese VPNs als „Krypto-VPNs“ bezeichnet werden.

Charakteristika von VPN-Verbindungen sind:

- VPNs werden als sichere Transportwege für schützenswerte Daten über ein nicht-vertrauenswürdiges Transportnetz verwendet.
- VPNs können berechtigte Zugriffe auf vertrauenswürdige Systeme auf sichere Weise ermöglichen und unberechtigte Zugriffe auf dieselben Systeme verhindern.
- VPNs können mit verschiedenen Technologien erzeugt werden.
- Der Einsatz von VPNs erfordert Schutzmaßnahmen für den VPN-Kanal und auch für die beteiligten Endpunkte.
- Die durch VPNs verbundenen Rechner und Netze können nicht prinzipiell als vertrauenswürdig eingestuft werden, so dass der Datenverkehr zu kontrollieren ist. Szenarien können beispielsweise die Einbindung von mobilen Mitarbeitern in das organisationsinterne Netz oder die Fernwartung durch Dritte darstellen.

Die technischen Probleme bei Verschlüsselung und Authentifizierung sind weitestgehend gelöst, d. h. es treten in der Regel keine gößeren Komplikationen auf, falls VPNs in Betrieb genommen werden sollen. Demgegenüber gibt es jedoch noch relativ wenig Informationen über die Integration von VPN-Komponenten in Sicherheitsgateways, z. B. Vor- und Nachteile verschiedener Platzierungen innerhalb eines Sicherheitsgateways oder Informationen über das Zusammenspiel verschiedener VPN-Produkte mit anderen Komponenten des Sicherheitsgateways.

1.1 Ziel und Inhalte der Studie

Gegenstand der vorliegenden Studie ist die sichere Integration von VPN-Komponenten in Sicherheitsgateways. Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und

hardwaretechnischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsrichtlinie ordnungsgemäß definierten Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden. Zudem können mit Sicherheitsgateways die übertragenen Daten kontrolliert werden.

Sicherheitsgateways bestehen abhängig von der Sicherheitseinstufung des nicht-vertrauenswürdigen Netzes aus verschiedenen Komponenten. Das BSI bietet zum Aufbau von Sicherheitsgateways die Studie „Konzeption von Sicherheitsgateways“ (siehe http://www.bsi.bund.de/) an, die Vor- und Nachteile verschiedener Grundstrukturen sowie Vor- und Nachteile der verschiedenen Platzierungsvarianten der modularen Erweiterungen des Sicherheitsgateways auflistet. Beispiele für Module sind Intrusion-Detection-Systeme (IDS), Virenscanner und Loghosts. Die vorliegende Studie versteht sich als Erweiterung der „Konzeption von Sicherheitsgateways“, indem für das Modul „VPN“ Vor- und Nachteile verschiedener Platzierungen betrachtet werden.

Am Übergang zwischen vertrauenswürdigen und nicht-vertrauenswürdigen Netzen sind häufig bereits Sicherheitsgateways installiert. Bei der Planung von VPNs muss deshalb die Integration der VPN-Endpunkte in ein Sicherheitsgateway berücksichtigt werden. Die Studie umfasst deshalb Informationen, wie der Schutz der beteiligten Rechner und Netze und des verwendeten Transportkanals entwickelt werden kann, wobei die Verwundbarkeit der vertrauenswürdigen Netze, des Transportkanals und der Vertrauensgrad der angeschlossenen Partner berücksichtigt werden. VPNs können damit je nach Sicherheitsansprüchen und -randbedingungen integriert werden.

Als Einführung und zur Darstellung des Themenhintergrundes werden zunächst grundlegende Aspekte wie Einsatzszenarien, Arten der Absicherung, kryptographische Grundlagen und VPN-Techniken beschrieben. Dabei werden wichtige Verschlüsselungsverfahren und Authentisierungsmechanismen behandelt. Dies soll helfen, grundsätzliche Fragestellungen und Probleme bei der Integration eines VPN-Gateways zu lösen. Die dann folgende Analyse der Platzierungsvarianten innerhalb eines Netzübergangs bildet einen wesentlichen Schritt bei der Integration eines VPN-Gateways in eine bestehende Infrastruktur.

Zur Unterstützung und Strukturierung einer VPN-Architektur werden die relevanten Anforderungen in Checklisten dargestellt. Diese Checklisten können dazu verwendet werden, abhängig vom Einsatzszenario und der Wahl der Krypto-Variante und Authentisierungsmethode eine Produktentscheidung zu treffen.

Da diese Studie hauptsächlich die Integration von VPN-Komponenten in Sicherheitsgateways betrachtet, werden ausschließlich Krypto-VPNs behandelt.

1.2 Inhaltsübersicht

In Kapitel 2 wird als Einführung in Virtual Private Networks zunächst die Funktionsweise der VPN-Techniken beschrieben. Das Kapitel enthält typische Einsatzszenarien für VPNs und die möglichen Varianten zur Netzkopplung. Für die Netzkopplungen wird beschrieben, welche Sicherheitsanforderungen an die Identifikation und Authentisierung der Kommunikationspartner und die Datenflusskontrolle bestehen.

Gängige Authentisierungsverfahren werden in Kapitel 3 erläutert und sicherheitstechnisch bewertet.

Die Funktionsweisen und die Vor- und Nachteile der aktuellen VPN-Techniken werden in Kapitel 4 detailliert beschrieben. Der Schwerpunkt liegt hierbei bei SSL und IPSec, es werden jedoch auch VPN-Techniken wie L2TP over IPSec behandelt.

Das Kapitel 6 behandelt die sichere Integration von VPN-Komponenten in Sicherheitsgateways und beschreibt die Möglichkeiten und die Vor- und Nachteile bei der Platzierung der VPN-Komponenten.

Kapitel 7 umfasst Empfehlungen zu Schutzmaßnahmen, wobei sich diese im Wesentlichen auf die Kriterien Identifikation/Authentisierung, Datenflusskontrolle, Beweissicherung, Übertragungssicherung und Schlüsselmanagement beziehen.

Kapitel 8 beschreibt wichtige VPN-Funktionen, die von einem VPN-Produkt bereitgestellt werden müssen, damit der Einsatz in speziellen Szenarien technisch überhaupt möglich ist. Hierunter fallen Funktionen wie Adressumsetzung und der Betrieb des VPN-Gateways mit mehreren Schnittstellen.

Kapitel 9 beschreibt verschiedene Aufbauformen von VPN-Produkten.

Die Entscheidungskriterien in Kapitel 10 sollen bei der Auswahl der richtigen Verschlüsselungs- und Authentisierungsmethode unterstützen. Die Vorschläge berücksichtigen unterschiedliche Szenarien und Krypto-Techniken.

In Anlage 1 befindet sich eine Checkliste, die bei der Beschaffung von VPN-Geräten die richtige Produktwahl erleichtern soll. In Anlage 2 befinden sich Verweise auf relevante VPN-Standards und -drafts, sowie in Anlage 3 ein Abkürzungsverzeichnis. In Anlage 4 werden die kryptographischen Grundlagen behandelt.

2. VPN-Tutorial

In Kapitel 2 werden Virtual Private Networks differenziert betrachtet: Im folgenden Unterkapitel werden zunächst verschiedene organisatorische Nutzungsszenarien vorgestellt. Das darauffolgende Unterkapitel umfasst die Gruppierung von VPNs anhand der unterschiedlichen Kommunikationspartner, die an Virtual Private Networks beteiligt sein können.

2.1 Typische VPN-Nutzungsszenarien

Nachfolgend werden die relevanten Einsatzszenarien beschrieben. Je nach Einsatzszenario sind beim Einsatz von VPNs funktionale Einschränkungen und Sicherheitsanforderungen zu berücksichtigen. Die Unterschiede bei der Realisierung der Szenarien werden in Kapitel 5 bei der Integration der VPN-Komponenten in Sicherheitsgateways berücksichtigt.

2.1.1 Mobiler Mitarbeiter

Ein mobiler Mitarbeiter benötigt u. U. einen Fernzugriff auf Daten, die sich nicht lokal auf dem verwendeten Rechner befinden, sondern auf einem Server innerhalb der Organisation. Bei der Absicherung solcher Verbindungen ist problematisch, dass sich der Mitarbeiter von wechselnden Arbeitsorten, z. B. einem Hotel oder Flughafen, mit dem internen Netz der Organisation verbinden möchte. Bei dem Client-System des Mitarbeiters handelt es sich meistens um ein Laptop, das zwar unter eigener Kontrolle steht, aber als nicht-vertrauenswürdig gelten sollte, da sich prinzipiell Unberechtigte einen Zugang zum Laptop verschaffen können.

Aus Kostengründen ist es gegenüber der direkten Einwahl in der Organisation oft sinnvoller, den mobilen Mitarbeiter unter Nutzung verfügbarer IP-Netze anzubinden. Diese IP-Netze sind meist unsichere, öffentliche Transportnetze – den Hauptanwendungsfall dürfte die Nutzung des Internets als Transportmedium darstellen. Da bei der Nutzung des Internets zur Anbindung an das vertrauenswürdige Netz schutzwürdige Daten über einen unsicheren Transportkanal übertragen werden, muss der Kanal geeignet abgesichert werden.

Bei diesem Szenario sind die folgenden Faktoren zu berücksichtigen (als das zur Übertragung genutzte Netz wird beispielhaft das Internet gewählt, die Anmerkungen gelten analog für jedes nicht-vertrauenswürdige Netz):

- Das Client-System besitzt evtl. bei unterschiedlichen Verbindungsversuchen unterschiedliche IP-Adressen.
- Nicht nur der Transportkanal, sondern auch das Endsystem selbst muss besonders abgesichert werden. Der Standort des Systems ist nicht kontrollierbar, und das Client-System kann kompromittiert werden, wenn es neben der VPN-Nutzung auch noch für andere Zwecke im Internet genutzt wird („Split-Tunneling“). Die Absicherung kann so gestaltet werden, dass das entfernte System bei bestehender VPN-Verbindung exklusiv in das interne Netz eingebunden wird. Hierbei gehen alle abgehenden Datenpakete des Clients in den Tunnel, und es werden ausschließlich Datenpakete aus dem Tunnel akzeptiert.
- Ein mobiles Client-System kann leicht in falsche Hände geraten. Der Aufbau des VPN-Tunnels sollte daher nicht automatisiert, sondern erst nach einer starken Authentisierung des Nutzers erfolgen.

2.1.2 Heimarbeitsplatz

Bei der Anbindung eines Heimarbeitsplatzes greift ein Client-System von einem festen Arbeitsort auf das interne Netz einer Organisation zu. Hierbei kann davon ausgegangen werden, dass der Heimarbeitsplatz ein integraler Bestandteil eines privaten LAN ist. Falls der Heimarbeitsplatz beispielsweise durch einen dedizierten VPN-Router vom Rest eines privaten LAN getrennt ist, so ist dieses Szenario eher mit einer „Standortvernetzung“ zu vergleichen.

Die Kommunikation erfolgt über unsichere, öffentliche Netze. Das System des Heimarbeitsplatzes kann entweder zentral oder vom Nutzer selbst administriert werden. Da die Räumlichkeiten zwar geschützt, die Nutzung des Systems jedoch nicht vollständig kontrolliert werden kann, ist das Client-System als bedingt vertrauenswürdig einzustufen.

Innerhalb der Studie steht die Anbindung des Heimarbeitsplatzes über das Internet im Vordergrund. Je nach Standort kann auch eine Direkteinwahl zum Ortstarif aus Kostengründen sinnvoll sein. Für beide Fälle ist eine geeignete Absicherung mittels Krypto-VPNs zu realisieren.

Bei diesem Szenario sind die folgenden Faktoren zu berücksichtigen:

- Das Client-System befindet sich üblicherweise mit wechselnden IP-Adressen im Internet, es sei denn, man nutzt einen DSL-Zugang mit einer festen IP-Adresse.
- Auch bei einem Heimarbeitsplatz muss nicht nur der Transportkanal, sondern auch das Client-System selbst abgesichert werden. Die Nutzung des Client-Systems ist nicht vollständig kontrollierbar, und das Client-System kann kompromittiert werden, wenn es neben der VPN-Nutzung auch noch für andere Zwecke im Internet genutzt wird.
- Obwohl die Räumlichkeiten geschützt sind, sollte der Tunnelaufbau zwischen dem Client-System und dem internen Netz nicht automatisiert ablaufen. Beispielsweise könnten unbefugte Familienmitglieder während einer kurzen Abwesenheit des Mitarbeiters Zugriff auf interne Daten erhalten.
- Der Zugriff sollte nur nach einer starken Authentisierung des Nutzers erlaubt werden.

2.1.3 Standortvernetzung

Bei der Standortvernetzung einer Organisation werden vertrauenswürdige Netze unter eigener Kontrolle über ein unsicheres öffentliches Transportnetz miteinander verbunden. In diesem Szenario ist besonders der Transportkanal abzusichern. Es wird davon ausgegangen, dass die Netze und die Client-Systeme der Standorte mittels Sicherheitsgateways gegen Angriffe aus dem Internet gesichert sind. In der Regel besitzen die VPN-Gateways feste IP-Adressen.

2.1.4 WLAN-Absicherung

Bei der Nutzung von WLAN-Technologien (“Wireless Local Area Network”) werden Zugriffe von Client-Systemen über ein potenziell schwach gesichertes Funknetz in das interne Netz einer Organisation ermöglicht. In diesem Szenario ist besonders der Transportkanal und das Client-System abzusichern. Das Transportnetz wird von der Organisation selbst betrieben, durch die beschränkten Mechanismen zur Zugriffskontrolle ist diese Technologie jedoch angreifbar.

Es muss berücksichtigt werden, dass das Client-System nur als bedingt vertrauenswürdig eingestuft werden kann. Die Nutzung des Client-Systems ist nicht kontrollierbar, so dass z. B. neben der WLAN-Verbindung gleichzeitig Verbindungen mit weiteren Netzen bestehen können, über die das Client-System angegriffen werden kann.

Abgesehen von der Absicherung des Transportkanals ist daher auch eine starke Authentisierung zu implementieren.

2.1.5 Kunden- und Partner-Anbindung

Die Anbindung von Kunden und Partnern an das interne Netz einer Organisation ist ein Sonderfall der im Kapitel 2.1.3 vorgestellten Standortvernetzung und häufig erforderlich, um den Ablauf von Betriebsprozessen zu gewährleisten. Hierzu gehören z. B. die folgenden Szenarien:

- Bereitstellung interner Informationen (initiiert aus dem nur eingeschränkt vertrauenswürdigen Netz, d. h. von „außen“)
- Abfrage externer Datenbanken (z. B. „Schufa“-Abfragen, initiiert aus dem vertrauenswürdigen Netz, d. h. von „innen“)
- Softwareentwicklung auf internen Systemen durch externe Firmen (initiiert aus dem nur eingeschränkt vertrauenswürdigen Netz, d. h. von „außen“)

Bei der Anbindung von Kunden und Partnern handelt es sich um die Verbindung von Netzen mit festen Standorten und Adressen. Die genutzten Dienstleistungen werden zwar vertraglich festgelegt, jedoch ist das entfernte Netz nicht unter eigener Kontrolle (betriebsfremdes Umfeld) und somit nicht uneingeschränkt vertrauenswürdig. Als Transportkanal wird häufig ein öffentliches, unsicheres Netz verwendet.

2.1.6 Fernwartung

Bei der Durchführung von Fernwartungstätigkeiten sind privilegierte Administratorzugänge auf interne Systeme erforderlich. Die Fernwartung (Wartung, Support und Betrieb) interner Systeme kann durch eigene oder fremde Mitarbeiter durchgeführt werden. In beiden Fällen bestehen daher hohe Anforderungen an die Authentisierung des entfernten Benutzers, die Datenflusskontrolle und die Verfügbarkeit der Anbindung.

Die Fernwartungsverbindungen können von Netzen mit festen Standorten oder mobilen Client-Systemen auf interne Systeme initiiert werden. Die genutzten Fernwartungsdienstleistungen werden zwar vertraglich festgelegt, jedoch ist das entfernte Netz bzw. System nicht unter eigener Kontrolle und somit nicht uneingeschränkt vertrauenswürdig. Als Transportkanal wird häufig ein öffentliches, unsicheres Netz verwendet.

2.2 Typische VPN-Realisierungen

VPNs müssen je nach Einsatzumgebung und Nutzungsszenario unterschiedlich realisiert werden, um die Anforderungen an die Sicherheit erfüllen zu können. Die folgenden Abschnitte beschreiben die Mechanismen für die Identifikation und Authentisierung der Kommunikationspartner und die Datenflusskontrolle, die die verschiedenen Architekturen leisten können. Die Einschränkungen der Architekturen werden bei den Empfehlungen in Abschnitt 6.15 berücksichtigt.

2.2.1 Client-Server

Client-Server-Verbindungen werden meist für die Nutzung einzelner Anwendungen verwendet. Die Verbindungen lassen sich auf spezielle Systeme und Dienste beschränken.

Typische Verwendungen für Client-Server-Verbindungen sind:

- Fernwartung dedizierter Systeme, bei der Zugriffe auf Administratorebene erforderlich sind.
- Zugriffe auf einzelne Anwendungen oder Datenbanken. Hierbei sind Berechtigungen auf Administrator- bzw. Systemebene häufig nicht erforderlich.
- Zugriffe über Terminal-Server. Durch die Fernsteuerung eines entfernten Systems kann jede Anwendung genutzt werden. Berechtigungen auf Administrator- bzw. Systemebene sind häufig nicht erforderlich.

Für die Realisierung einer Client-Server-Anbindung existieren die folgenden Rahmenbedingungen:

Identifikation und Authentisierung

- Die Verbindung wird vom Client-System initiiert. Bei der Einwahl in das Internet erhält das Client-System eine beliebige IP-Adresse, so dass die Identität des Systems nicht über die IP-Adresse verifizierbar ist. Aufgrund der Manipulierbarkeit ist die Authentisierung anhand der IP-Adresse als alleiniges Kriterium ohnehin nicht empfehlenswert.
- Die Authentisierung kann zwischen den VPN-Partnern, z. B. über eine Kombination von IP-Adresse und festem Kennwort („Shared Secret“), durchgeführt werden. Diese Art der Authentisierung ist nicht möglich, wenn sich die IP-Adresse bei jeder Einwahl ändert.
- Da sich das Client-System in einem Umfeld befindet, das nicht unter der Kontrolle der Organisation steht, ist eine Authentisierung des Benutzers gegenüber dem Betriebssystem nicht ausreichend, um eine VPN-Verbindung zu erlauben.

Datenflusskontrolle

- Bei einer Client-Server-Verbindung auf Netzebene sind zunächst alle Anwendungen erreichbar, die vom Server angeboten werden. Dies betrifft unter Umständen auch die Dienste, die die Administration des Servers erlauben. Bei der Anbindung eines Clients ist es deshalb erforderlich, dass der Zugriff auf den Server auf die zur Aufgabenerledigung erforderlichen Dienste eingeschränkt wird.

2.2.2 Client-LAN

Client-LAN-Verbindungen werden für Zugriffe des Client-Systems auf mehrere Anwendungen auf unterschiedlichen Systemen im LAN einer Organisation verwendet. Es wird ein Zugriff auf das gesamte Netz benötigt. Der Transportkanal wird durch VPN-Software auf dem Client-System und einem VPN-Gateway im LAN gesichert.

Eine typische Verwendung für Verbindungen zwischen Clients und LANs ist die Anbindung von Telearbeitsplätzen oder mobilen Mitarbeitern.

Für die Realisierung einer Client-LAN-Anbindung existieren die folgenden Rahmenbedingungen:

Identifikation und Authentisierung

- Die Verbindung wird vom Client-System initiiert. Bei der Einwahl in das Internet erhält das Client-System eine beliebige IP-Adresse, so dass die Identität des Systems nicht über die IP-Adresse verifizierbar ist. Aufgrund der Manipulierbarkeit ist die Authentisierung anhand der IP-Adresse als alleiniges Kriterium ohnehin nicht empfehlenswert.
- Die Authentisierung kann zwischen den VPN-Partnern, z. B. über eine Kombination von IP-Adresse und festem Kennwort („Shared Secret“), durchgeführt werden. Diese Art der Authentisierung ist nicht möglich, wenn sich die IP-Adresse bei jeder Einwahl ändert.
- Da sich das Client-System in einem Umfeld befindet, das nicht unter der Kontrolle der Organisation steht, ist eine Authentisierung des Benutzers gegenüber dem Betriebssystem nicht ausreichend, um eine VPN-Verbindung zu erlauben.

Datenflusskontrolle

- Bei einer Client-LAN-Verbindung sind grundsätzlich alle Systeme des internen Netzes erreichbar. Es ist technisch sicherzustellen, dass das Client-System nur Verbindungen mit internen Systemen initiieren kann, die für die durchzuführenden Tätigkeiten erforderlich sind.
- Die Nutzung der bereitgestellten Anwendungen sollte kontrolliert werden.

2.2.3 LAN-LAN

Mit LAN-LAN-Verbindungen werden Netze gekoppelt, um gemeinsame Anwendungen betreiben bzw. nutzen zu können. Es werden netzübergreifende Zugriffe benötigt. Der Transportkanal wird durch VPN-Gateways in den angeschlossenen Netzen gesichert.

Eine typische Verwendung für Verbindungen zwischen LANs ist die Anbindung von Filialen oder Partnerfirmen an das organisationsinterne Netz.

Für die Realisierung einer LAN-LAN-Anbindung existieren die folgenden Rahmenbedingungen:

Identifikation und Authentisierung

- Die Kommunikationspartner besitzen feste IP-Adressen, so dass die Authentisierung auf Basis einer Kombination von IP-Adresse und festem Kennwort technisch möglich ist.
- Falls die Rechner, die zum Zugriff auf das jeweils andere LAN verwendet werden, unter der eigenen Kontrolle stehen, ist eine Authentisierung des Benutzers gegenüber dem Betriebssystem ausreichend, um eine eingehende Verbindung zu erlauben. Dies gilt beispielsweise nicht bei der Anbindung von Partnerfirmen.

Datenflusskontrolle

- Bei einer LAN-LAN-Verbindung sind grundsätzlich alle Systeme der verbundenen Netze erreichbar. Es ist sicherzustellen, dass Client-Systeme nur Verbindungen mit internen Systemen initiieren können, die für die durchzuführenden Tätigkeiten erforderlich sind.
- Die Nutzung der bereitgestellten Anwendungen sollte kontrolliert werden.

3. Sichere Authentisierung von VPN-Komponenten

Die Authentisierung ist eine der wichtigsten Sicherheitsfunktionen bei der Planung, der Konfiguration und dem Betrieb von VPNs. Im Folgenden werden die gängigen Authentisierungsverfahren erläutert und sicherheitstechnisch bewertet. Die notwendigen kryptographischen Grundlagen werden in Anlage 4 erläutert.

3.1 Verwendung von statischen Schlüsseln

In zahlreichen VPN-Implementierungen gibt es die Möglichkeit, feste Schlüssel für die symmetrische Verschlüsselung zu nutzen. Die Authentisierung erfolgt dabei indirekt, da nur Entitäten mit Zugang zum Schlüssel die Kommunikation entschlüsseln können. Werden innerhalb der Verschlüsselung Prüfsummen der Klartext-Nachricht versandt, kann der Empfänger nachvollziehen, ob der Sender sich im Besitz des Schlüssels befindet.

Die Verwendung statischer Schlüssel birgt große Sicherheitsnachteile. Die Schlüssel bleiben meist für lange Zeiträume unverändert und dienen somit zur Verschlüsselung von großen Datenmengen. Dies erleichtert die Kryptoanalyse der verschlüsselten Daten und ermöglicht eine langzeitige Nutzung der gebrochenen Verschlüsselung.

Ein weiteres Problem stellt der Übertragungsweg der verschlüsselungsrelevanten Informationen dar. Die Schlüssel, die verwendeten Algorithmen und die Parameter müssen über Übertragungswege ausgetauscht werden, die vom geplanten VPN unabhängig sind. Es muss also bereits ein sicherer Kanal oder eine andere Austauschmöglichkeit vorhanden sein.

Eine höhere Sicherheit bietet die Entkopplung der Authentisierungsinformation von der eigentlichen Verschlüsselung, da die ausgetauschten Authentisierungsdaten relativ klein sind. Zudem bietet sich die Möglichkeit einer dynamischen Schlüsselgenerierung. Alle in den folgenden Abschnitten beschriebenen Verfahren nutzen diese Möglichkeit.

3.2 Pre-Shared Keys

Ein Pre-Shared Key (PSK; auch Shared Secret genannt) ist ein geheimer Schlüssel, der beiden Kommunikationspartnern vor Beginn des Authentisierungsverfahrens zur Verfügung stehen muss. PSK müssen selbst während der Authentisierung nicht übertragen werden. Die meisten PSK-Verfahren basieren auf dem Versand von Hash-Werten, berechnet aus dem PSK und einem von der Gegenstelle zugesandten Nonce (Challenge). Dies verhindert Wiederholungsattacken, da der Nonce von dem überprüfenden System erzeugt wird und eine Wiederholung seines Werts extrem unwahrscheinlich ist.

Die Authentisierung kann maschinen- oder personenbezogen erfolgen:

Bei der machinenbezogenen Authentisierung wird der PSK im Klartext oder verschleiert abgespeichert. Verschleiert heißt in diesem Zusammenhang, dass aus der abgespeicherten Form des PSK ohne zusätzliche Informationen die Klartextform des PSK nicht abgeleitet werden kann. Das kann z. B. bedeuten, dass der PSK mit einem in der VPN-Software fest programmierten Schlüssel symmetrisch verschlüsselt wurde.

Im Falle der personenbezogenen Authentisierung muss der Schlüssel von der zu authentisierenden Person eingegeben werden, oder der Schlüssel befindet sich verschlüsselt auf einem Speichermedium und kann nur mit dem von der Person eingegebenen Passwort entschlüsselt werden.

Ähnlich der Authentisierung durch statische Schlüssel besitzt die PSK-Authentisierung den Nachteil, dass der PSK auf einem sicheren Weg auf die Kommunikationsteilnehmer übertragen werden muss. Dafür muss bereits ein sicherer Kanal vorhanden sein.

Ein weiterer Nachteil besteht darin, dass idealerweise pro Authentisierungspartnerpaar ein individueller PSK verwendet werden sollte. In der Praxis wird oft ein einziger PSK für die ganze VPN-Infrastruktur verwendet, was die Sicherheit erheblich beeinträchtigt.

Ferner kann die Wahl des PSKs Einfluss auf die Sicherheit haben, da triviale PSKs anfällig gegen Wörterbuchattacken sind.

3.3 Public-Key-Verfahren, Zertifikate

Mit Public-Key-Verfahren können Authentisierungen sowohl mit Public-Key-Signierung als auch mit Public-Key-Verschlüsselung realisiert werden:

Bei der häufiger anzutreffenden Authentisierung mittels Signierung (s. Anlage 4.3) wird der Hash-Wert des von der Gegenstelle zugesandten Nonce mit Hilfe des privaten Schlüssels signiert und an die Gegenstelle zurückgeschickt. Die Authentizität kann die Gegenstelle mit dem öffentlichen Schlüssel der zu authentisierenden Instanz überprüfen.

Dieses Verfahren ist nicht-abstreitbar. Nicht-Abstreitbarkeit („non-repudiation“) bedeutet, dass die ausgetauschten Authentisierungsdaten zum Nachweis der Beteiligung der Entitäten am Authentisierungsprozess genutzt werden können.

Bei der Authentisierung mittels Public-Key-Verschlüsselung wird der Nonce mit dem öffentlichen Schlüssel der zu authentisierenden Instanz verschlüsselt und an diese versandt. Diese antwortet ebenfalls mit einem verschlüsselten Nonce. Nach einer erfolgreichen Entschlüsselung auf beiden Seiten verfügen die Kommunikationsparteien über zwei Nonces, die zur Ableitung eines Sitzungsschlüssels genutzt werden können.

Dieses Verfahren ist abstreitbar, d. h., die ausgetauschten Authentisierungsdaten können nicht zum Nachweis der Beteiligung der Entitäten am Authentisierungsprozess genutzt werden.

Die Authentisierung kann maschinen- oder personenbezogen erfolgen:

Bei einer machinenbezogenen Authentisierung wird der private Schlüssel im Klartext oder verschleiert abgespeichert oder befindet sich z. B. auf einer SmartCard ohne PIN (Persönliche Identifikationsnummer). Eine weitere Möglichkeit ist die Benutzung einer SmartCard mit PIN, wobei die PIN im Klartext oder verschleiert auf dem System abgespeichert wird.

Im Falle der personenbezogenen Authentisierung befindet sich der private Schlüssel verschlüsselt auf einem Speichermedium und kann mit dem von der Person eingegebenen Passwort entschlüsselt werden, wie z. B. bei einer SmartCard mit einer dem Benutzer bekannten PIN.

Die Zuordnung der öffentlichen Schlüssel zum Kommunikationspartner wird meist anhand eines Zertifikats durchgeführt. Um den aktuellen Gültigkeitsstatus eines Zertifikats festzustellen, ist meist eine Einbettung der VPN-Knoten in eine PKI notwendig.

3.4 Einmalpasswörter

Einmalpasswörter („One-Time-Passwords“) verlieren nach einer Verwendung ihre Gültigkeit. Somit wird gewährleistet, dass ein Abhören einer Authentisierungssitzung einem Angreifer keine Informationen bereitstellt, die diesem eine spätere Authentisierung ermöglichen könnten. Die einfachste Form eines

Einmalpassworts bilden Einmalpasswortlisten, welche vor allem beim Internet-Banking als TANs (Transaktionsnummern) Anwendung finden.

Interessanter für VPN-Anwendungen sind Einmalpasswörter, die von kleinen Kryptogeräten erzeugt werden, die an die zu authentisierenden Benutzer ausgegeben werden. Die Geräte beinhalten einen internen Timer sowie einen PSK in einer nicht auslesbaren Form. Aus dem Timer-Wert und dem PSK wird mit Hilfe eines Hash-Algorithmus das Einmalpasswort generiert, das eine begrenzte Lebensdauer besitzt. Bei einigen Geräten werden Einmalpasswörter laufend angezeigt. Eine zweite Variante besitzt ein numerisches Eingabefeld für die Eingabe einer PIN. Hier wird erst nach einer erfolgreichen PIN-Eingabe das zu dieser Zeit gültige Einmalpasswort angezeigt.

Der Authentisierungsserver verfügt über eine Kopie des PSK und über einen Timer, der synchron mit dem Gerätetimer ist. So kann er das jeweils gültige Passwort errechnen und dies mit der Benutzereingabe vergleichen. Da die in der Praxis verwendeten Timer kleine Gangunterschiede aufweisen, muss ein Mechanismus verwendet werden, der bei jeder Anmeldung den Servertimer mit dem Gerätetimer synchronisiert. Dabei muss auf dem Server pro verwaltetes Gerät ein individueller Timer geführt werden.

Der Authentisierungsserver befindet sich meist nicht auf dem VPN-Server bzw. VPN-Gateway selbst. Das Einmalpasswort und der Benutzername werden von dem VPN-Server bzw. VPN-Gateway an den Authentisierungsserver weitergeleitet. Dieser antwortet mit dem Ergebnis der Passwort-Überprüfung. Die Verbindung zwischen dem VPN-Server bzw. VPN-Gateway und dem Authentisierungsserver muss bezüglich der Authentizität der Kommunikationspartner und der Integrität sowie der Vertraulichkeit der ausgetauschten Daten abgesichert sein.

Die Einmalpasswort-Authentisierung erfolgt meist nur einseitig, d. h., der Benutzer des VPN-Clients authentisiert sich gegenüber dem VPN-Server bzw. dem VPN-Gateway. Die Authentisierung in die entgegengesetzte Richtung erfolgt meist mit anderen Methoden, z. B. zertifikatsbasiert.

3.5 Challenge-Response-Verfahren

Beim Challenge-Response-Verfahren werden die Passwörter asynchron aus einem PSK und einem vom Authentisierungsserver zugesandten Nonce erzeugt. Dies hat den Vorteil, dass keine Timer synchronisiert werden müssen. Der Nachteil des Verfahrens besteht darin, dass die Zusendung einer Nonce im Rahmen einiger älterer Anmeldeprotokolle nicht möglich ist.

Wie das Einmalpasswort-Verfahren dient das Challenge-Response-Verfahren lediglich einer einseitigen Authentisierung des VPN-Clients am VPN-Server bzw. VPN-Gateway. Die Authentisierung in die entgegengesetzte Richtung erfolgt meist mit anderen Methoden, z. B. zertifikatsbasiert.

3.6 Vergleich der Authentisierungsverfahren

Die folgende Tabelle gibt eine Zusammenfassung der wichtigsten Eigenschaften der in diesem Kapitel beschriebenen Authentisierungsverfahren. Ferner wird in der Tabelle eine grobe Einschätzung der Verfahren bezüglich ihrer Sicherheit vorgenommen, die unter bestimmten Einzelaspekten betrachtet möglicherweise nicht zutreffend ist. Somit ist im jeweiligen Anwendungszusammenhang eine Einzelbewertung der Sicherheit des Authentisierungsverfahrens unbedingt erforderlich. Die grobe Einschätzung geht von der Anwendung starker Kryptoalgorithmen in den Verfahren aus.

Grundlegend ist zu der Ordnung der Verfahren folgendes zu sagen:

Verfahren mit Passwort/PIN sind den Verfahren ohne Passwort/PIN vorzuziehen, d. h., Besitz und Wissen ist sicherer als Besitz allein.

Einmalpasswörter sind unveränderlichen Passwörtern vorzuziehen, da bei Einmalpasswörtern ein Wiedereinspielen nicht möglich ist.

Pre-Shared Keys sind den statischen Schlüsseln vorzuziehen, da bei Pre-Shared Keys relativ geringe Datenmengen ausgetauscht werden und somit die Kryptoanalyse erschwert wird.

Einmalpasswörter sind insofern mit den Challenge-Response-Verfahren gleichzusetzen, als beide auf der Grundlage eines PSK arbeiten, lediglich die Ableitung der Passwörter geschieht mit unterschiedlichen Verfahren.

Methode	**personenbezogen**	**maschinenbezogen**	**einseitig**	**Authentisierungsmerkmal**				**Reihenfolge bzgl. der Sicherheit der einzelnen Verfahren (1=niedriger, 8=höher)**
				gespeichert	**Wissen**	**Besitz**	**kopierbar**	
Statische Schlüssel		x		x			x	1
PSK im Klartext		x		x			x	2
PSK verschleiert		x		x			x	3
PSK-Eingabe durch Benutzer	x				x		x	3
PSK passwortgeschützt	x			x	x		x	3
Public Key (Privater Schlüssel im Klartext)		x		x			x	4
Public Key (Privater Schlüssel verschleiert)		x		x			x	5
Public Key (Privater Schlüssel passwortgeschützt)	x			x	x	(x) [1)]	x	5
Public Key (Privater Schlüssel auf SmartCard ohne PIN)		x				x		6
Public Key (Privater Schlüssel auf SmartCard mit PIN)	x				x	x		8
Einmalpasswörter (als Liste)	x	x	x	x			x	7
Einmalpasswörter auf Geräten ohne PIN		x	x			x	(x) [2)]	7
Einmalpasswörter auf Geräten mit PIN	x		x		x	x	(x) [2)]	8
Challenge Response Geräte ohne PIN		x	x			x	(x) [2)]	7
Challenge Response Geräte mit PIN	x		x		x	x	(x) [2)]	8

Tabelle 1: Authentisierungsverfahren. Die Betrachtung der Sicherheit der einzelnen Verfahren ist allgemeiner Art und muss im jeweiligen Anwendungszusammenhang unbedingt gesondert verglichen bzw. betrachtet werden. Starke Kryptoalgorithmen werden in der allgemeinen Betrachtung vorausgesetzt.

Anmerkungen zur Tabelle:

[1)] Falls auf einem externen Medium abgespeichert.

[2)] Da die Geräte meist auf einem PSK-Verfahren basieren, muss ein Schlüsselaustausch zwischen dem Gerät und dem Authentisierungsserver möglich sein. Das Auslesen des Schlüssels aus dem Gerät selbst ist jedoch in den meisten Fällen nicht möglich.

4. Krypto-VPN-Varianten

Im Folgenden werden die wichtigsten Technologien bzw. Protokolle vorgestellt, mit denen VPNs erzeugt werden können.

Die meisten der in diesem Kapitel vorgestellten Protokolle wurden durch die „Internet Engineering Task Force“ (IETF) standardisiert und als „Requests for Comments“ (RFC) veröffentlicht. Die folgenden Ausführungen beschränken sich auf die wichtigsten Grundlagen. Weitergehende Informationen finden sich in den RFC, die in der Anlage 2 aufgelistet werden.

4.1 Internet Protocol Security (IPSec)

„Internet Protocol Security“ (IPSec) ist die zurzeit in der Wirtschaft und Verwaltung am weitesten verbreitete VPN-Implementierung. Unter IPSec versteht man eine Reihe von Protokollen zur Schlüsselverwaltung und zur Authentisierung und Verschlüsselung. IPSec ist für das Internet-Protokoll in der Version 6 (IPv6) obligatorisch, bei der Version 4 (IPv4) kann es optional implementiert werden. IPSec bietet eine für den Benutzer weitgehend transparente Verbindung von Rechnersystemen.

Im Folgenden werden die technischen Grundlagen von IPSec erläutert.

4.1.1 Verschlüsselung und Paketstruktur

Die IPSec-Spezifikationen definieren zwei IP-Protokolle:

- Encapsulating Security Payload (ESP) für die Verschlüsselung und Authentisierung
- Authentication Header (AH) für die Authentisierung

Da ESP auch ohne Verschlüsselung und somit zur reinen Authentisierung verwendet werden kann, ist der Einsatz von AH nicht sehr weit verbreitet.

Beide Protokolle unterstützen den Tunnel-Mode und den Transport-Mode:

- Im Tunnel-Mode werden die IP-Pakete mitsamt Header verschlüsselt. Da der Tunnel-Mode sich für RAS-Szenarios sowie Kopplungen zwischen zwei Netzen eignet, findet er in der Praxis die größere Verbreitung als der Transport-Mode.
- Im Transport-Mode wird der IP-Header der Ursprungspakete übernommen, verschlüsselt wird lediglich der Paket-Inhalt. Dieser Modus eignet sich nur für Kommunikationen, bei denen die Tunnelendpunkte gleichzeitig die Kommunikationsendpunkte darstellen, also beispielsweise bei einer direkten Client-Server-Kommunikation ohne Proxies.

Der Unterschied zwischen beiden Modi wird im Folgenden jeweils am Beispiel von ESP und AH erläutert. Die Daten der Ursprungspakete sind dabei jeweils grau hinterlegt.

4.1.1.1 Tunnel- und Transportmodus bei Encapsulating Security Payload (ESP)

Abbildung 1 stellt ein Beispielpaket nach der ESP-Verschlüsselung im Tunnel-Mode dar. Das Paket wird mitsamt IP-Header verschlüsselt.

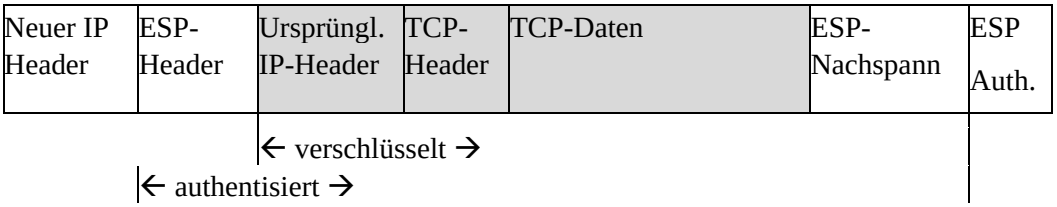


Abbildung 1 Beispielpaket nach der ESP-Verschlüsselung im Tunnel-Mode

In der Abbildung 2 wird das Beispielpaket nach einer ESP-Verschlüsselung im Transport-Mode dargestellt. Der IP-Header wird in diesem Fall nicht verschlüsselt und wird als IP-Header des ESP-Pakets verwendet.

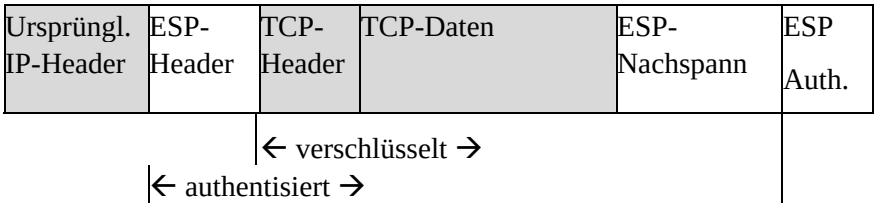


Abbildung 2 Beispielpaket nach der ESP-Verschlüsselung im Transport-Mode

4.1.1.2 Tunnel- und Transportmodus bei Authentication Header (AH)

Abbildung 3 und Abbildung 4 zeigen die Unterschiede beim Tunnel- bzw. Transport-Mode bei einer AH-Kapselung des Beispielpakets. Zu beachten ist, dass im Gegensatz zu ESP hier das ganze AH-Paket einschließlich seines IP-Headers bis auf die veränderlichen Header-Teile authentisiert wird.

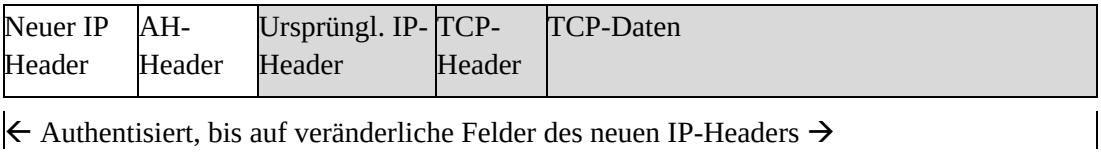


Abbildung 3 Beispielpaket nach der AH-Kapselung im Tunnel-Mode

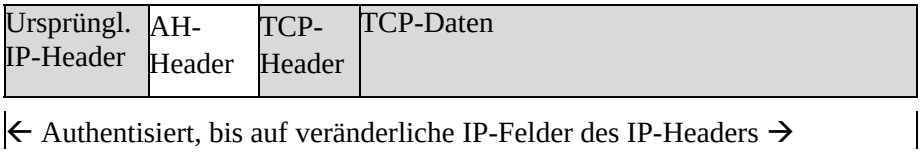


Abbildung 4 Beispielpaket nach der AH-Kapselung im Transport-Mode

4.1.2 Einordnung im ISO/OSI-Schichtenmodell

Mit Hilfe von IPSec können IP-Pakete als ESP- bzw. AH-Pakete in der dritten ISO/OSI-Schicht transportiert werden (vgl. Abbildung 5).

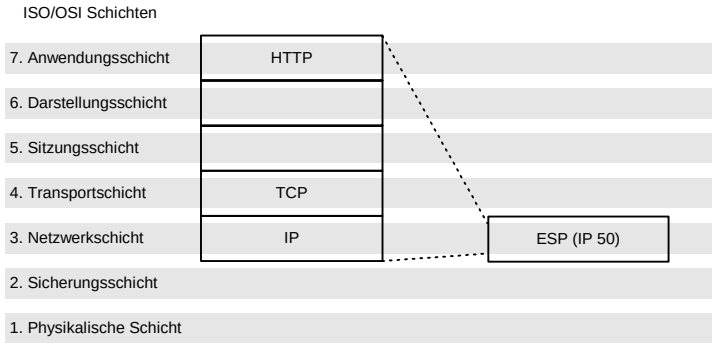


Abbildung 5 IPSec im ISO/OSI-Schichtenmodell

Bei einer UDP-Kapselung von ESP (s. auch 4.1.5) werden die Pakete, wie in Abbildung 6 gezeigt, in der vierten ISO/OSI-Schicht transportiert.

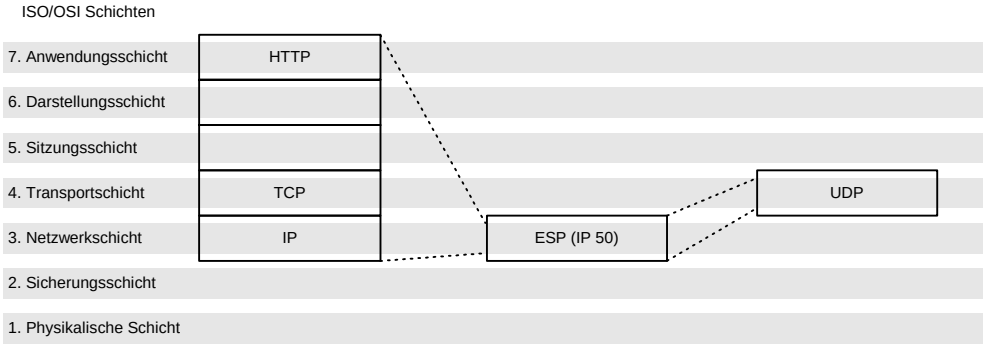


Abbildung 6 UDP-Kapselung von IPSec

4.1.3 Grundlagen der Schlüsselverwaltung bei IPSec

RFC 2401 sieht die Implementierung von zwei Datenbanken vor, der Security Policy Database (SPD) und der Security Association Database (SAD). Bei den meisten Implementierungen handelt es sich hierbei nicht um eine Datenbank, sondern um geordnete Listen, die im Hauptspeicher abgelegt und verwaltet werden.

Die SPD enthält Einträge mit Sicherheitsvorgaben für beispielsweise Quell- und Ziel-Adresse, IP-Protokollnummer und Portnummer. Diese Einträge sind verknüpft mit Anweisungen zum Verwerfen, Weiterleiten oder zum Verschlüsseln. Die für die Verschlüsselung zuständigen Einträge der SPD beinhalten zusätzlich Informationen für die Security Association (SA). Die SA beschreibt die Beziehung zwischen zwei oder mehr Entitäten und charakterisiert die zum Schutz der ausgetauschten Daten benutzten Verfahren und deren Parameter.

Anhand der SPD-Einträge wird für jedes ankommende und ausgehende Paket entschieden, wie es verarbeitet wird. Da Pakete ggf. auch verworfen werden müssen, ist bei jeder IPSec-Implementierung ein einfacher Paketfilter erforderlich.

Entspricht ein Paket einem SPD-Eintrag für Verschlüsselung, so wird – soweit noch nicht geschehen – eine SA aufgebaut und als Eintrag in der SAD abgelegt. Diesem SPD-Eintrag wird dann ein Verweis auf diesen SAD-Eintrag hinzugefügt, so dass folgende Pakete entsprechend der SA verschlüsselt werden können. Nach dem Abbau der SA wird der entsprechende Eintrag aus der SAD entfernt.

Vor der eigentlichen Verschlüsselung müssen sich die Kommunikationspartner über die zu verwendende SA einig sein. In vielen IPSec-Implementierungen gibt es die Möglichkeit, mit statischen SA und Schlüsseln zu arbeiten. Dies ist jedoch mit den in 3.1 beschriebenen Nachteilen verbunden. Eine dynamische Aushandlung von SA und Schlüsseln ist beispielsweise mit dem “Internet Key Exchange Protocol” möglich.

4.1.4 Internet Key Exchange Protokoll (IKE)

Das Internet Key Exchange Protokoll (IKE) ermöglicht eine dynamische Aushandlung der SA und der Schlüssel für die IPSec-Verschlüsselung. Es basiert auf dem „Internet Security Association and Key Management Protocol“ (ISAKMP), das lediglich ein Framework für Schlüsselaustauschverfahren darstellt, aber diese nicht selber definiert.

IKE gliedert sich in folgende zwei Phasen:

1. Phase 1 dient der Aushandlung einer „ISAKMP Security Association“, die einen authentifizierten, verschlüsselten Kanal darstellt. Dies kann entweder im Main Mode oder im Aggressive Mode erfolgen. Die Modi unterscheiden sich durch die Anzahl der auszutauschenden Nachrichten und die Verschlüsselung der ausgetauschten Daten:

   - Main Mode: Sechs Nachrichten werden ausgetauscht, die Identitätsinformationen werden verschlüsselt.
   - Aggressive Mode: Drei Nachrichten werden ausgetauscht, die Identitätsinformationen werden nicht verschlüsselt. Eine Ausnahme stellt der Aggressive Mode mit Public-Key-Verschlüsselung als Authentisierungsmethode dar.
     Der Agressive Mode ist schneller, aber unsicherer als der Main Mode.

2. In Phase 2 werden die SAs und Schlüssel ausgehandelt, mit denen ein Sicherungsprotokoll wie IPSec – oder jegliches andere Protokoll, das Schlüsselmaterial benötigt – arbeiten soll.

Die IKE-Spezifikation definiert folgende Authentisierungsmethoden:

- Pre-Shared Keys (PSK),
- Public-Key-Signaturen,
- Public-Key-Verschlüsselung und
- Revidierte Public-Key-Verschlüsselung.

Die letzten beiden Verfahren haben in der Praxis eine sehr geringe Verbreitung.

Im Folgenden wird die Phase-1-Kommunikation unter Benutzung dieser Authentisierungsmethoden näher erläutert. Ferner werden die ausgetauschten Nachrichten der Phase 2 dargestellt.

Folgende Bezeichnungen werden dabei benutzt, wobei *x* bzw. *X* für i bwz. I (Initiator-Daten) und r bzw. R (Responder-Daten) steht.

Abkürzung	Beschreibung
HDR	ISAKMP-Header
HDR*	ISAKMP-Header, wobei die folgenden Daten verschlüsselt sind (Die verschlüsselten Nachrichten werden zusätzlich grau unterlegt).
SAi, SAr	Security-Association-Daten mit einem oder mehreren Vorschlägen. Nur der Initiator kann mehrere Vorschläge senden (SAi). Der Responder antwortet immer mit einem Vorschlag (SAr).
KE	Öffentliche Key-Exchange-Daten des Diffie-Hellman-Exchange
Nx	Nonce
IDx	Identitätsdaten
HASH	Hash-Wert
SIG_X	Signierter HASH
Y_b	Y ohne den generischen ISAKMP-Header
PubKey_x	Public Key
CERT-X	Zertifikat
<Y>K	Y verschlüsselt mit dem Schlüssel K
[Y]	Y optional

Tabelle 2: Abkürzungsverzeichnis zur Beschreibung des IKE-Prozesses

4.1.4.1 Phase 1 mit Pre-Shared Keys

In Phase 1 mit PSK erfolgt die Authentisierung anhand vordefinierter Schlüssel, deren Verteilung über einen bereits vorhandenen, sicheren Kanal oder über andere Wege erfolgen muss.

Im Main Mode (s. Abbildung 7) sendet der Initiator als erstes eine SA-Vorschlagsliste (SA_i) mit einem oder mehreren Vorschlägen an den Responder. Dieser antwortet mit einem einzigen SA-Vorschlag (SA_r) aus der Vorschlagsliste des Initiators. Daraufhin sendet der Initiator die öffentlichen Key-Exchange-Daten (KEi) und den von ihm generierten Nonce (Ni). Der Responder antwortet mit seinen öffentlichen Key-Exchange-Daten (KEr) und dem von ihm generierten Nonce (Nr). Aus KEi, Ni, KEr und Nr sowie dem PSK können nun beide Parteien die symmetrischen Schlüssel für die Authentisierung und Verschlüsselung von ISAKMP und weiterer Protokolle ableiten.

Es folgt der verschlüsselte Austausch von Identitätsdaten (IDii und IDrr) und von Hash-Werten zur Authentisierung der ausgetauschten Daten.

Im Main Mode mit PSK ist lediglich die Nutzung von IP-Adressen als IDs sinnvoll, da der PSK aus der Security-Policy-Datenbank (SPD) für die Bildung des Schlüssels abgerufen werden muss, noch bevor der Identitäten-Austausch stattgefunden hat.

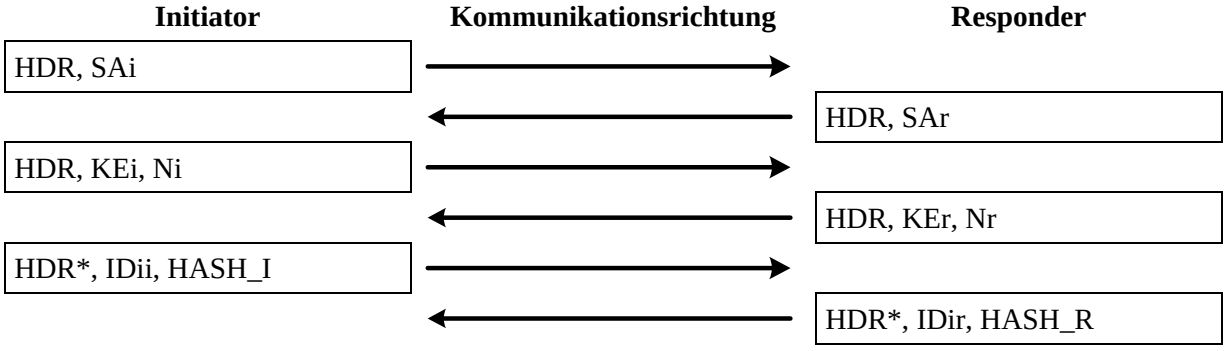


Abbildung 7 Main Mode mit PSK

Im Aggressive Mode werden die Identitätsinformationen im Klartext verschickt (s. Abbildung 8).

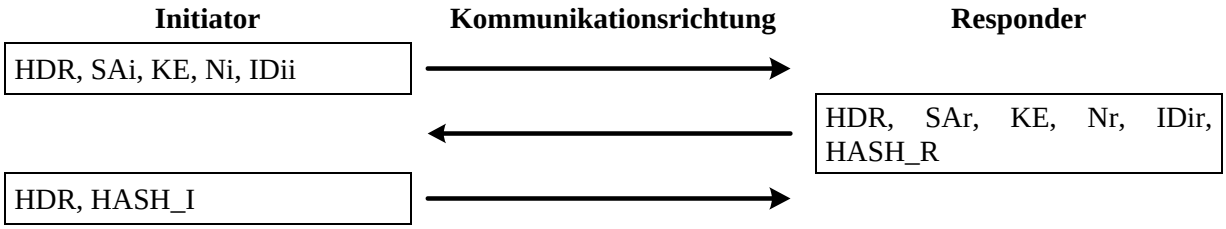


Abbildung 8 Aggressive Mode mit PSK

4.1.4.2 Phase 1 mit Public-Key-Signaturen

Die Authentisierung erfolgt anhand von elektronischen Signaturen, wobei die Kommunikationspartner über eigene, gültige Zertifikate mit den zugehörigen privaten Schlüsseln verfügen müssen.

Im Main Mode (s. Abbildung 9) sendet der Initiator zuerst eine SA-Vorschlagsliste (SA_i) mit einem oder mehreren Vorschlägen an den Responder. Dieser antwortet mit einem einzigen SA-Vorschlag (SA_r) aus der Vorschlagsliste des Initiators. Daraufhin sendet der Initiator die öffentlichen Key-Exchange-Daten (KEi) und den von ihm generierten Nonce (Ni). Der Responder antwortet mit seinen öffentlichen Key-Exchange-Daten (KEr) und dem von ihm generierten Nonce (Nr). Aus KEi, Ni, KEr und Nr können nun beide Parteien die symmetrischen Schlüssel für die Authentisierung und Verschlüsselung von ISAKMP und weiterer Protokolle ableiten.

Es folgt der verschlüsselte Austausch von Identitätsdaten (IDii und IDir) und von mit dem jeweiligen privaten Schlüssel des Absenders signierten Hash-Werten (SIG_I und SIG_R) zur Authentisierung der ausgetauschten Daten. Die Identitätsdaten müssen einem oder mehreren Einträgen des Zertifikats entsprechen. Optional können hier die (ebenfalls verschlüsselten) Zertifikate des Initiators und Responders ausgetauscht werden.

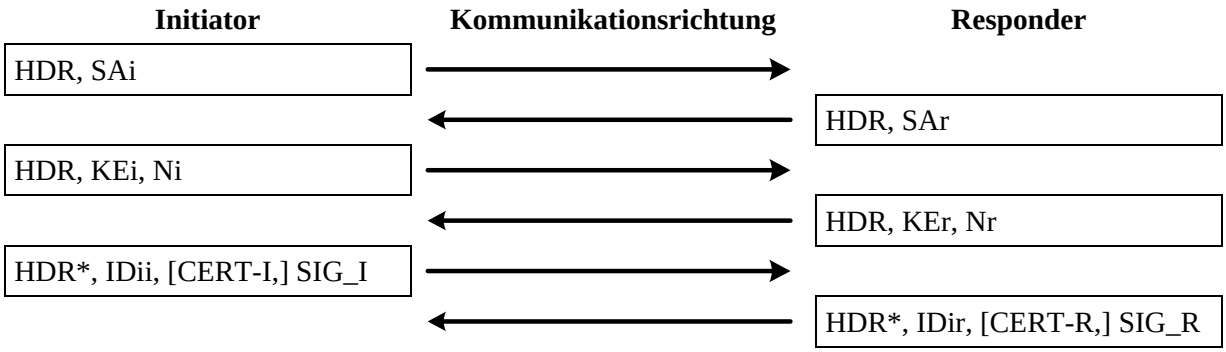


Abbildung 9 Main Mode mit Signaturen

Im Aggressive Mode werden die Identitäten und Signaturen (sowie optional Zertifikate) im Klartext übertragen (s. Abbildung 10).

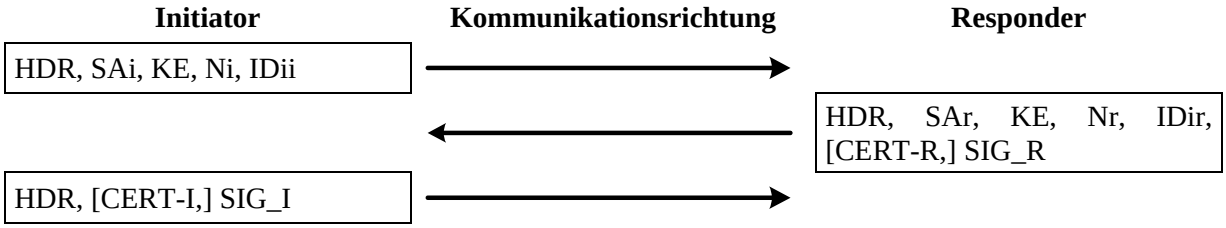


Abbildung 10 Aggressive Mode mit Signaturen

Wird die Phase 1 mit Hilfe von Signaturen (Zertifikaten) durchgeführt, so werden die ausgetauschten Authentifikationsinformationen mit Hilfe signierter Hash-Werte beglaubigt. Bei den beiden anderen Verfahren der Phase 1 (Pre-shared-Key und Public-Key-Verschlüsselung) werden dazu unsignierte Hash-Werte herangezogen. Nur das Signaturverfahren sichert daher Nichtabstreitbarkeit der Kommunikation.

4.1.4.3 Phase 1 mit Public-Key-Verschlüsselung

Bei der Authentisierung mit Public-Key-Verschlüsselung werden die Daten der ID-Informationen (IDii_b, IDir_b) sowie der Nonces (Ni_b und Nr_b) mit den öffentlichen Schlüsseln der Kommunikationspartner verschlüsselt. Sollten mehrere Zertifikate für den Kommunikationspartner vorhanden sein, wird der Hash-Wert des Zertifikats mitgeschickt, um eine Zertifikatsidentifizierung zu ermöglichen.

Diese Authentisierungsmethode ermöglicht im Vergleich zu der Authentifizierung mit Signaturen eine nicht-abstreitbare Kommunikation. Ferner erhöht sie die Sicherheit des Verfahrens, denn um die ausgehandelten Schlüssel zu erhalten, müsste ein Angreifer nicht nur den Diffie-Hellman-Austausch, sondern auch beide Public-Key-Verschlüsselungen brechen.

Abbildung 11 zeigt die im Main Mode ausgetauschten Informationen.

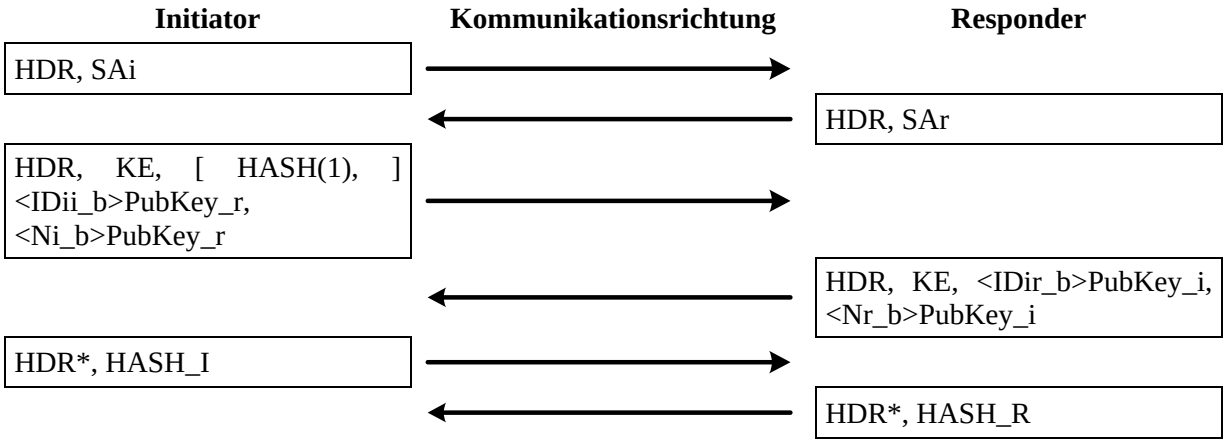


Abbildung 11 Main Mode mit Public-Key-Verschlüsselung

Im Gegensatz zu den bislang vorgestellten Verfahren werden die Identitätsinformationen im Aggressive Mode (s. Abbildung 12) kryptographisch geschützt.

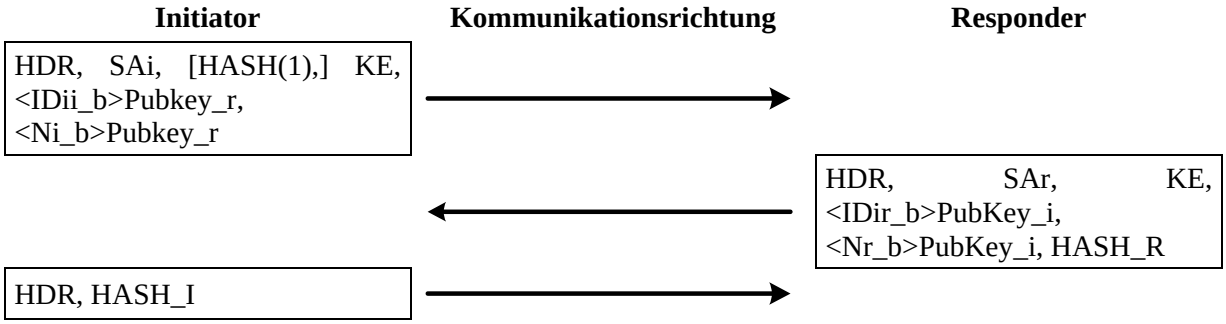


Abbildung 12 Aggressive Mode mit Public-Key-Verschlüsselung

4.1.4.4 Phase 1 mit revidierter Public-Key-Verschlüsselung

Um die Rechenintensität von vier Public-Key-Operationen pro Kommunikationspartner bei der zuletzt vorgestellten Authentisierungsmethode zu reduzieren, wurde ein weiteres Verfahren vorgeschlagen, in dem nur die Nonces mit dem Public Key verschlüsselt werden. Die Identitätsdaten (IDii) sowie zusätzlich die Key-Exchange-Daten (KE) werden symmetrisch mit einem aus dem Nonce (Ni bzw. Nr) abgeleiteten Schlüssel (Ke_i und Ke_r) verschlüsselt. Dies bietet einen zusätzlichen Schutz der Key-Exchange-Daten.

Abbildung 13 stellt die Main Mode Kommunikation dar.

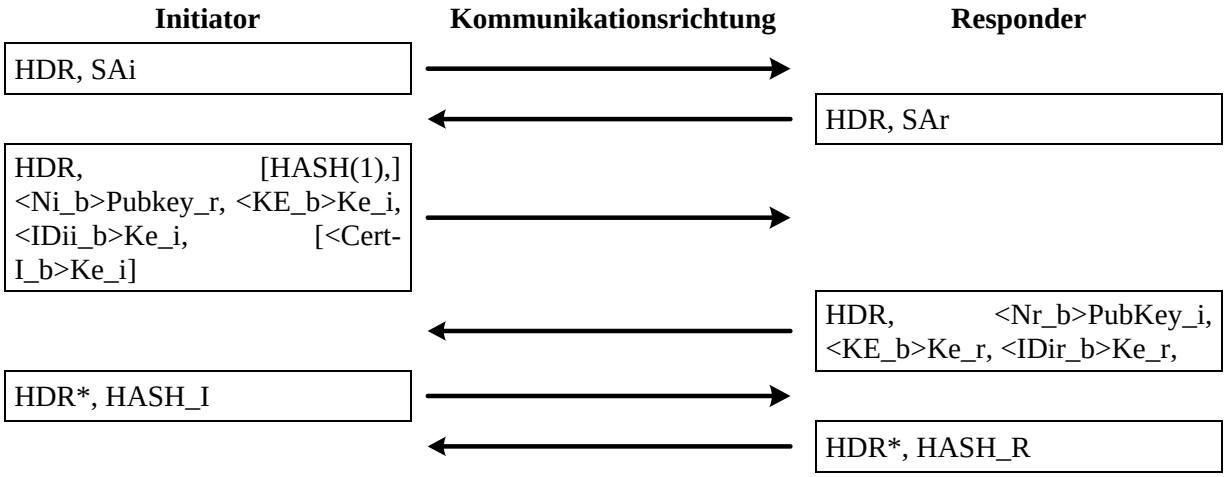


Abbildung 13 Main Mode mit revidierter Public-Key-Verschlüsselung

Im Aggressive Mode (s. Abbildung 14) werden wie bei der zuletzt vorgestellten Methode die Identitätsinformationen geschützt.

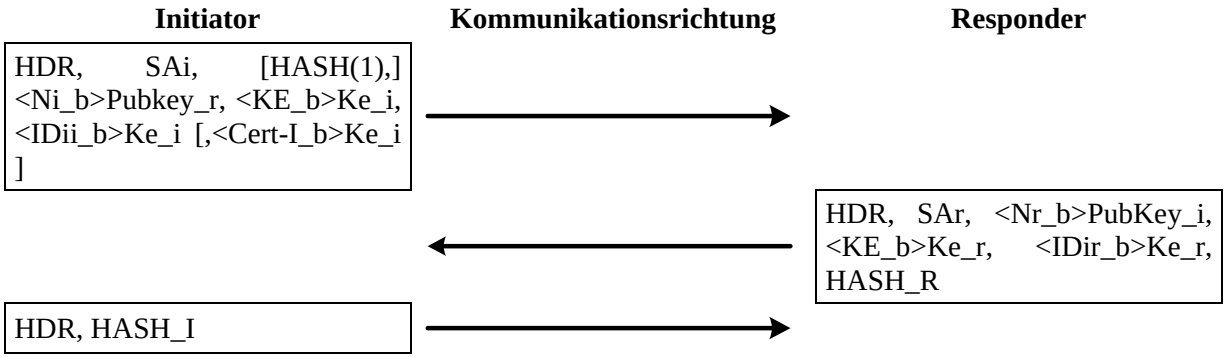


Abbildung 14 Aggressive Mode mit revidierter Public-Key-Verschlüsselung

4.1.4.5 Phase 2: Quick Mode

Die Phase 2 (s. Abbildung 15) dient dem Aufbau von SA für weitere Dienste wie ESP oder AH und wird durch die in der Phase 1 aufgebauten SA gesichert. Innerhalb von Phase 2 können mit derselben SA mehrere Quick Modes abgewickelt werden, z. B. für verschiedene Quell- und Zielnetze oder nach Ablauf des Timeouts der Phase-2-SA.

Es werden mindestens zwei SA für ein- und ausgehende Kommunikation ausgehandelt. Der Initiator sendet die SA-Vorschlagsliste (SA_i) mit einem oder mehreren Vorschlägen an den Responder. Dieser antwortet mit einem einzigen SA-Vorschlag (SA_r) aus der Vorschlagsliste des Initiators. Sollen mehrere SAs ausgehandelt werden, versendet der Initiator nicht eine, sondern mehrere Vorschlagslisten, die mit der gleichen Anzahl an Vorschlägen beantwortet werden.

Die ausgetauschten Nonces dienen zur Ableitung des Schlüsselmaterials. Ist auch in dieser Phase Perfect Forward Secrecy erwünscht, gibt es die Möglichkeit, einen zusätzlichen Key-Exchange (KE) durchzuführen.

Wenn keine Identitätsinformationen (IDci und IDcr) ausgetauscht werden, werden die IP-Adressen der Peers als Identitätsnachweis verwendet.

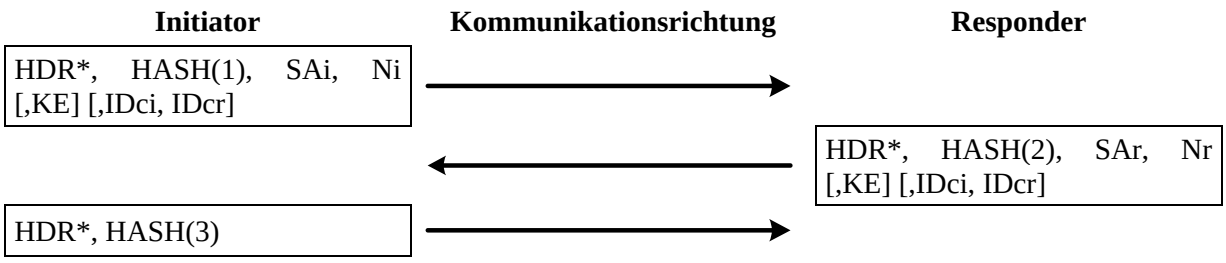


Abbildung 15 Quick Mode

4.1.5 Umgang mit Network Address Translation (NAT-Traversal)

Im Folgenden wird lediglich auf die NAT-Variante Bezug genommen, bei der mehrere IP-Adressen eines privaten Netzes mit einer öffentlichen IP-Adresse ersetzt werden. Die folgenden Probleme stellen nur einen Auszug dar, weitere Szenarien finden sich in RFC 3715:

- Das AH-Protokoll ist grundsätzlich inkompatibel mit der NAT, da bei AH die Adressen im IP-Header authentisiert werden. Eine Veränderung der IP-Adressen würde die Überprüfung der Authentizität an der Gegenstelle fehlschlagen lassen.
- Bei ESP im Transport-Modus befinden sich die TCP- oder UDP-Checksummen innerhalb der verschlüsselten Daten und können vom NAT-Gateway nicht neu gesetzt werden, ohne die Gültigkeit der Checksumme zu verletzen und damit das Verwerfen der Pakete an der Gegenstelle zu provozieren. Zudem sind die zur Checksummenbildung herangezogenen Header-Daten ebenfalls verschlüsselt.
- Da ESP keine Ports verwendet, ist in einem Szenario, in dem zwei oder mehr VPN-Knoten aus dem internen Netz über NAT mit einem externen VPN-Knoten kommunizieren, kein Demultiplexing von ESP möglich, d. h., Antwortpakete können dem ursprünglichen Initiator der Verbindung nicht mehr zugeordnet werden. Ähnliches gilt für die IKE-Kommunikation über reine NAT-Gateways.
- Auch bei NAT-Gateways kann es in Verbindung mit IKE zu Problemen kommen, wenn das System im öffentlichen Netz bei IKE-Kommunikation den Quellport 500/UDP erwartet. Deshalb verwenden manche NAT-Gateways bei Kommunikation über 500/UDP reines NAT (“Basic NAT”), bei dem nur die IP-Adresse ersetzt wird, was wiederum zu Demultiplexing-Problemen führen kann.
- In Protokollen, die auf der Anwendungsebene IP-Adressen beinhalten (wie z. B. File Transfer Protocol [FTP], Simple Network Management Protocol [SNMP]) können bei der Verschlüsselung der Pakete die IP-Adressen in den höheren Protokollschichten am NAT-Gateway nicht verändert werden. Somit können ESP-geschützte Protokolle nicht oder nur eingeschränkt über NAT verwendet werden.

Seit Jahren wird an der Problematik des NAT-Traversals in der IPSec Working Group des IETF gearbeitet. Die Ergebnisse hierzu sind noch offen. Viele Hersteller von VPN-Software haben daher in ihren Produkten eine oder mehrere Versionen der z. T. untereinander inkompatiblen Lösungsvorschläge implementiert.

4.1.6 Interoperabilitätsproblematik

Nicht alle IPSec-Implementierungen bieten die gleichen Merkmale. Lediglich folgende Merkmale sind für eine RFC-konforme IPSec-Implementierung zwingend erforderlich:

- Verschlüsselungsalgorithmus: Data Encryption Standard (DES) im CBC-Mode (“Cipher Block Chaining”)
- Hash-Funktionen: Message Digest Algorithm 5 (MD5) und Secure Hash Algorithm (SHA)

- Authentisierung: PSK
- Oakley-Gruppe für den Diffie-Hellman-Austausch: 1 (768 bit)
- Main Mode

Trotz einer vom Hersteller zugesicherten Kompatibilität zu einem Dritthersteller-Produkt kann deshalb u. U. lediglich eine Kommunikation auf einem sehr niedrigen Sicherheitsniveau möglich sein, z. B. mittels PSK-Authentisierung und schwacher Verschlüsselung.

Weitere Probleme stellen sich wie folgt dar:

- Um die Interoperabilität zu gewährleisten, müssen beide Kommunikationspartner den gleichen Identifizierungstyp verwenden. IKE sieht jedoch für die Phase 1 verschiedene Identifizierungstypen vor, die nicht von allen VPN-Produkten unterstützt werden. In vielen Produkten sind die benutzten Typen zudem nicht eindeutig erkennbar.
- VPN-Produkte können unterschiedliche Vorgaben bezüglich der zu verwendenden Zertifikatsfelder besitzen. Es ist darauf zu achten, dass die eingesetzten Zertifikate von beiden Kommunikationspartnern verwendet werden können.
- Nicht standardisierte Passwort-Verfahren wie Extended Authentication und Hybrid Authentication werden nicht von allen Produkten unterstützt.
- Da der Standardisierungsprozess für NAT-Traversal noch nicht abgeschlossen ist, verfügen Produkte evtl. über keine oder untereinander inkompatible Implementierungen des NAT-Traversals (s. auch 4.1.5).
- Nicht alle Hersteller halten sich an die RFC-Vorgaben bezüglich der Fragmentierung von ESP-Paketen, so dass möglicherweise ein Kommunikationspartner fragmentierte ESP-Pakete verwirft.

In jedem Fall ist die Kompatibilität der interoperierenden Komponenten im Hinblick auf die geforderten Funktionalitäten vor einer Produkteinführung zu überprüfen. Diese Prüfung sollte über das reine Zustandekommen des Tunnels auf einem den Vorgaben entsprechenden Sicherheitsniveau auch den Austausch von überlangen Paketen, mehrfaches Re-Keying von Phase 1 und Phase 2, Lasttests sowie Tests der für die VPN-Nutzung geplanten Applikationen enthalten. Die Prüfungen sollten nicht nur lokal mit VPN-Client und VPN-Gateway im gleichen LAN, sondern in möglichst realitätsnahen Umgebungen stattfinden, z. B. mittels Internetverbindung über einen DSL-Router über einen öffentlichen Hot-Spot.

4.1.7 Benötigte Paketfilterregeln

Für den IPSec-Verkehr müssen an den beteiligten Sicherheitsgateways die Dienste IKE, ESP und ggf. AH freigeschaltet werden (s. Tabelle 3). In den folgenden Tabellen beziehen sich Quellport und Zielport auf den Initiator der Verbindung.

Dienst	Protokoll	Quellport	Zielport
IKE	UDP (IP 17)	nicht festgelegt	500
ESP	IP 50	entfällt	entfällt
AH	IP 51	entfällt	entfällt

Tabelle 3: Standard-IPSec-Dienste

Bei Implementationen nach den NAT-T-Draft-Versionen 0 und 1 sind keine zusätzlichen Freischaltungen erforderlich, da die verschlüsselte Kommunikation (ESP über UDP) über Port 500/UDP erfolgt (s. Tabelle 4).

Dienst	Protokoll	Quellport	Zielport
IKE	UDP (IP 17)	nicht festgelegt	500
ESP over UDP	UDP (IP 17)	nicht festgelegt	500
ESP	IP 50	entfällt	entfällt

Tabelle 4 IPSec-Dienste nach NAT-T-Version 0 und 1

NAT-T Draft-Versionen 2 und höher werden, falls NAT erkannt wird, die IKE-Verhandlungen über Port 4500/UDP fortsetzen. Die verschlüsselte Kommunikation (ESP over UDP) erfolgt über Port 4500/UDP (s. Tabelle 5).

Dienst	Protokoll	Quellport	Zielport
IKE	UDP (IP 17)	nicht festgelegt	500, 4500
ESP over UDP	(IP 17)	nicht festgelegt	4500
ESP	IP 50	entfällt	entfällt

Tabelle 5 IPSec-Dienste nach NAT-T-Version 2 und höher

Im Folgenden werden Beispielregelwerke für den Linux-Paketfilter IPTables zu verschiedenen Szenarien gegeben.

Im ersten Szenario dürfen alle Clients eines LANs auf ein VPN-Gateway oder einen VPN-Server außerhalb des LANs zugreifen. Das LAN wird durch einen Linux-Paketfilter gesichert. Die mit der Variable $INNEN bezeichnete Netzschnittstelle dieses Paketfilters ist mit dem LAN verbunden. Die Schnittstelle mit der Bezeichnung $AUSSEN ist mit dem äußeren Netz verbunden. Zusätzlich können die Verbindungen auf ein einziges VPN-Gateway beschränkt werden. Dessen IP-Adresse wird mit der Variablen $VPNGW bezeichnet.

Dienst	IPTables-Regeln
IKE [1)] ESPoUDP [2)]	iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN [--dst $VPNGW] --dport 500 --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN [--src $VPNGW] --sport 500 --m state --state ESTABLISHED,RELATED -j ACCEPT
ESP [1)]	iptables -A FORWARD -p 50 -i $INNEN -o $AUSSEN [--dst $VPNGW] --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p 50 -i $AUSSEN -o $INNEN [--src $VPNGW] --m state --state ESTABLISHED,RELATED -j ACCEPT
AH	iptables -A FORWARD -p 51 -i $INNEN -o $AUSSEN [--dst $VPNGW] --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p 51 -i $AUSSEN -o $INNEN [--src $VPNGW] --m state --state ESTABLISHED,RELATED -j ACCEPT
IKE [3)] ESPoUDP [3)]	iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN [--dst $VPNGW] --dport 4500 --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN [--src $VPNGW] --sport 4500 --m state --state ESTABLISHED,RELATED -j ACCEPT

Erläuterungen zur Tabelle:

Betrifft Standard-IPSec und alle NAT-T-Drafts.

Betrifft NAT-T-Versionen 0 und 1.

Betrifft NAT-T-Versionen 2 und höher.

Das zweite Szenario stellt das andere Kommunikationsende des ersten Szenarios dar. Hierbei wird das VPN-Gateway von einem Linux-Paketfilter geschützt. Die mit der Variablen $INNEN bezeichnete Netzschnittstelle dieses Paketfilters ist mit dem gleichen lokalen Netz verbunden wie die äußere Netzschnittstelle des VPN-Gateways. Die Schnittstelle mit der Bezeichnung $AUSSEN ist mit dem äußeren Netz verbunden. Die IP-Adresse des VPN-Gateways wird mit der Variablen $VPNGW bezeichnet.

Dienst	**IPTables-Regeln**
IKE [1)] ESPoUDP [2)]	iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN --dst $VPNGW --dport 500 --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN --src $VPNGW --sport 500 --m state --state ESTABLISHED,RELATED -j ACCEPT
ESP [1)]	iptables -A FORWARD -p 50 -i $AUSSEN -o $INNEN --dst $VPNGW --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p 50 -i $INNEN -o $AUSSEN --src $VPNGW --m state --state ESTABLISHED,RELATED -j ACCEPT
AH	iptables -A FORWARD -p 51 -i $AUSSEN -o $INNEN --dst $VPNGW --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p 51 -i $INNEN -o $AUSSEN --m state --state ESTABLISHED,RELATED -j ACCEPT
IKE [3)] ESPoUDP [3)]	iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN --dst $VPNGW --dport 4500 --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN --src $VPNGW --sport 4500 --m state --state ESTABLISHED,RELATED -j ACCEPT

Erläuterungen zur Tabelle:

1) Betrifft Standard-IPSec und alle NAT-T-Drafts.

2) Betrifft NAT-T-Versionen 0 und 1.

3) Betrifft NAT-T-Versionen 2 und höher.

Das dritte Szenario beinhaltet eine LAN-LAN-Kopplung zwischen zwei VPN-Gateways: VPNGW1 und VPNGW2. Hier werden lediglich die Regeln für den Linux-Paketfilter vor VPNGW1 angegeben. Die Regeln für den Paketfilter vor VPNGW2 sind analog.

Die mit der Variablen $INNEN bezeichnete Netzschnittstelle ist mit dem gleichen lokalen Netz verbunden wie die äußere Netzschnittstelle des VPNGW1. Die Schnittstelle unter der Variablen $AUSSEN ist mit dem äußeren Netz verbunden. Die IP-Adressen der VPN-Gateways werden mit den Variablen $VPNGW1 und $VPNGW2 bezeichnet. Da die Verbindungen in diesem Szenario von beiden Seiten initiiert werden können, ist eine Statefull Inspection nicht sinnvoll.

Dienst	IPTables-Regeln
IKE [1)] ESPoUDP [2)]	iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN --src $VPNGW1 --dst $VPNGW2 --sport 500 --dport 500 -j ACCEPT iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN --src $VPNGW2 --dst $VPNGW1 --sport 500 --dport 500 -j ACCEPT
ESP [1)]	iptables -A FORWARD -p 50 -i $INNEN -o $AUSSEN --src $VPNGW1 --dst $VPNGW2 -j ACCEPT iptables -A FORWARD -p 50 -i $AUSSEN -o $INNEN --src $VPNGW2 --dst $VPNGW1 -j ACCEPT
AH	iptables -A FORWARD -p 51 -i $INNEN -o $AUSSEN --src $VPNGW1 --dst $VPNGW2 -j ACCEPT iptables -A FORWARD -p 51 -i $AUSSEN -o $INNEN --src $VPNGW2 --dst $VPNGW1 -j ACCEPT
IKE [3)] ESPoUDP	iptables -A FORWARD -p UDP -i $INNEN -o $AUSSEN --src $VPNGW1 --dst $VPNGW2 --sport 4500 --dport 4500 -j ACCEPT iptables -A FORWARD -p UDP -i $AUSSEN -o $INNEN --src $VPNGW2 --dst $VPNGW1 --sport 4500 --dport 4500 -j ACCEPT

Erläuterungen zur Tabelle:

1) Betrifft Standard-IPSec und alle NAT-T-Drafts.

2) Betrifft NAT-T-Versionen 0 und 1.

3) Betrifft NAT-T-Versionen 2 und höher.

4.1.8 Checklisten zur sicheren IPSec-Konfiguration

Im Folgenden werden Checklisten zur sicheren IPSec-Konfiguration gegeben.

Anforderung	erfüllt	
	ja	nein
Der Schlüsselaustausch ist mit einem sicheren Verfahren mit ausreichender Schlüssellänge durchgeführt worden (ISAKMP-Group 2 oder besser 5).		
Sichere Verschlüsselungsverfahren mit ausreichender Schlüssellänge werden verwendet (Advanced Encryption Standard 128 [AES-128], 3DES).		
Hash-Algorithmen mit ausreichender Länge werden verwendet (SHA-1, Race Integrity Primitives Evaluation Message Digest 160 [RIPEMD-160]).		
Sichere Authentisierungsverfahren werden verwendet (vgl. Kapitel 3).		
Timeouts der Phasen 1 und 2 sind nicht zu groß gewählt.		
Es ist darauf verzichtet worden, PSK als Authentifizierungsmethode zu verwenden (insbesondere in Client-Gateway-Szenarien).		
Falls verwendet, wurden für PSK sichere Schlüssel gewählt.		

Anforderung	erfüllt	
	ja	nein
Bei Verwendung von XAUTH wurde die Authentizität des Responders (VPN-Gateway, VPN-Server) mit sicheren Methoden festgestellt.		

Tabelle 6: Sichere IPSec-Konfiguration (allgemein)

Speziell für VPN-Clients sollten zusätzlich folgende Anforderungen erfüllt sein:

Anforderung	erfüllt	
	ja	nein
Authentisierungsschlüssel (PSK, Private Key) werden nur verschlüsselt auf dem System gespeichert.		
Für den Schutz der Authentisierungsschlüssel wurde ein komplexes Passwort gewählt.		
Direkte Verbindungen außerhalb des Tunnels zu nicht-vertrauenswürdigen Systemen (“Split-Tunneling”) werden während einer VPN-Sitzung vollständig unterbunden.		
Clientsysteme genügen dem sonst im Organisationsnetz üblichen Schutzniveau bezüglich dem Schutz vor Viren und Trojanischen Pferden.		
Clientsysteme werden bei direkter Verbindung mit nicht-vertrauenswürdigen Netzen (auch bei inaktivem VPN) durch einen Paketfilter gesichert.		
Sämtliche Patches sind installiert.		

Tabelle 7 Sichere IPSec-Konfiguration der Clients

An die VPN-Gateways werden zusätzlich folgende Anforderungen gestellt:

Anforderung	erfüllt	
	ja	nein
Bei Verwendung von Zertifikaten zur Authentisierung wird während jedes Authentisierungsvorgangs der Status des Zertifikats bei der PKI überprüft.		
Es sind keine IPSec-fremden Dienste auf der äußeren Netzschnittstelle aus dem nicht-vertrauenswürdigen Netz erreichbar.		
IPSec-Verbindungen werden lediglich zu den notwendigen Systemen und Diensten erlaubt.		
Die im internen Netz sichtbaren IP-Adressen der sich verbindenden VPN-Clients stammen aus einem beschränkten Adressenbereich. [1)]		

Tabelle 8 Sichere IPSec-Konfiguration der VPN-Gateways

1) Dies ist z. B. bei direkten Einwahlverbindungen gegeben. Ist dies nicht der Fall, wie z. B. bei der Einwahl über einen Provider, sollten den sich verbindenden VPN-Clients IP-Adressen aus einem internen Pool

zugeordnet werden (NAT am VPN-Gateway), damit eine Filterung am internen Sicherheitsgateway nach Quelladressen möglich ist.

4.1.9 Häufig auftretende Probleme und deren Behebung

Die wichtigsten Hilfsmittel zur Problemlösung stellen die Protokollierungsfunktion sowie die Fehlermeldungen der IPSec-Implementierung dar. Diese sind jedoch bei verschiedenen Produkten sehr unterschiedlich ausgeprägt. Oft kann der Detaillierungsgrad der Fehlermeldungen eingestellt werden. Für die Lösung eines Problems ist es sinnvoll, temporär den Detaillierungsgrad zu erhöhen. Im täglichen Betrieb sollte dieser moderat bleiben, um Ressourcen zu schonen und die Performance nicht unnötig zu vermindern. Ein weiteres Hilfsmittel stellt ein Paketsniffer dar, dessen Einsatz sowohl auf dem VPN-Knoten selbst als auch in den beteiligten Transportnetzen sinnvoll sein kann. Manche IPSec-Produkte bieten einen integrierten Paketsniffer. Dies hat den Vorteil, dass Pakete sowohl in ihrem verschlüsselten als auch im unverschlüsselten Zustand dargestellt werden können.

Weitere Anhaltspunkte bieten Protokollierungsfunktionen der beteiligten Netzkomponenten wie Router und Sicherheitsgateways.

Die häufigsten Konfigurationsprobleme eines IPSec-VPNs sind auf disjunkte SA-Vorschlagslisten zurückzuführen, d. h., keiner der SA-Vorschläge des Initiators stimmt mit den Vorschlägen des Responders bezüglich Identifikationstypen, Authentisierungs-, Verschlüsselungs- und Komprimierungsverfahren und Timeouts überein. Dies kann sowohl in Phase 1 als auch in Phase 2 auftreten. Bei vielen Implementierungen werden die jeweils kleinsten Timeouts übernommen.

Um diese Probleme zu vermeiden, sollte insbesondere bei umfangreichen VPN-Installationen ein zentral administrierbares IPSec-Produkt verwendet werden, bei dem die Einstellungen der VPN-Clients, -Gateways und -Server an einer Stelle verknüpft vorgenommen werden können.

Ein weiterer Grund für das Scheitern einer IPSec-Verbindung sind oft ungenügende Freischaltungen auf Sicherheitsgateways. Die nötigen Paketfilterregeln werden in 4.1.7 erläutert.

Mit den vielfältigen Problemen, die bei Verwendung von IPSec durch NAT hervorgerufen werden können, beschäftigt sich der Abschnitt 4.1.5

Bei Anbindungen mit kleiner Bandbreite ist deren optimale Nutzung sehr wichtig. Diese wird oft mit Komprimierungsverfahren in der zweiten ISO/OSI-Schicht verbessert, was bei einer starken Verschlüsselung in der dritten ISO/OSI-Schicht scheitert. Mit der Bandbreiten-Problematik beschäftigt sich der Abschnitt 4.1.1.

4.2 Layer 2 Tunneling Protocol (L2TP) over IPSec

Die neueren Microsoft-Betriebssysteme (Windows 2000, XP und 2003 Server) beinhalten Komponenten zum Aufbau von VPNs mittels eines L2TP-Tunnels, der mit IPSec kryptographisch abgesichert wird. Die folgenden Abschnitte behandeln IPSec/L2TP/PPP als VPN-Komponente und die Besonderheiten der IPSec-Implementierung in der IPSec/L2TP-Suite.

Im weiteren Kontext dieser Studie wird zur Vermeidung von Missverständnissen folgende Sprachregelung getroffen:

- Der Begriff L2TP bezieht sich ausschließlich auf die Eigenschaften des L2TP-Protokolls. Dasselbe gilt für IPSec und PPP ("Point-To-Point-Protocol").
- L2TP/PPP umfasst Eigenschaften, die die Kombination beider Tunnelprotokolle beinhalten.
- IPSec/L2TP/PPP beschreibt schließlich den gesamten hier relevanten Protokollstack.

L2TP wurde als eigenständiges Protokoll aus den Vorgängern Point-to-Point-Tunneling-Protocol (PPTP, veraltetes VPN-Protokoll von Microsoft) und Layer-Two-Forwarding (L2F, proprietäres Protokoll von Cisco Systems) entwickelt und als RFC 2661 veröffentlicht. Ziel war es, ein einheitliches Protokoll zu schaffen, das es erlaubt, PPP-Pakete möglichst transparent für Endnutzer und Anwendungen über ein IP-Netz transportieren zu können.

4.2.1 L2TP-Grundlagen

Im folgenden Abschnitt wird zunächst allgemein erläutert, wie L2TP funktioniert und wozu es – auch außerhalb des IPSec-Kontextes – genutzt wird. Danach wird die im Kontext dieser Studie relevante Kombination von L2TP und IPSec behandelt. Schließlich wird die Struktur von L2TP-Nachrichten dargestellt.

4.2.1.1 Grundszenario

Ursprünglich wurde L2TP entwickelt, um PPP-Verbindungen über Access-Konzentratoren wie Modembänke oder Digital Subscriber Line Access Multiplexer (DSLAM) hinweg herstellen zu können. PPP-Verbindungen enden damit nicht notwendigerweise an den Access-Konzentratoren sondern können über diese hinweg geleitet werden. In der Terminologie von L2TP werden die Access-Konzentratoren, als LAC (L2TP Access Concentrator) und die PPP-Endpunkte als LNS (L2TP Network Server) bezeichnet.

Üblicherweise ist ein Access-Konzentrator auch gleichzeitig der Endpunkt des PPP-Kanals. Das Grundszenario für die Nutzung von L2TP sieht einen Nutzer vor, der sich bei einem Provider einwählt, um über diese Verbindungsstrecke mittels PPP ein Netzprotokoll, z. B. IP, Frame Relay oder ATM, nutzen zu können. Die Verbindung des Endgeräts zum Provider terminiert dort auf einem Access-Konzentrator. Vom Access-Konzentrator werden dann die über die Wählverbindung erhaltenen PPP-Pakete des Endgerätes mittels L2TP zu dem eigentlichen PPP-Endpunkt über irgendein Transfernetz weitergetunnelt.

Während also die Einwahlverbindung auf einem LAC terminiert, wird die eigentliche PPP-Verbindung zwischen dem Endgerät des Nutzers und dem LNS aufgebaut, wobei L2TP nur zwischen LAC und LNS zum Tragen kommt.

Die folgende Übersicht zeigt den L2TP-Tunnel zwischen LAC und LNS:

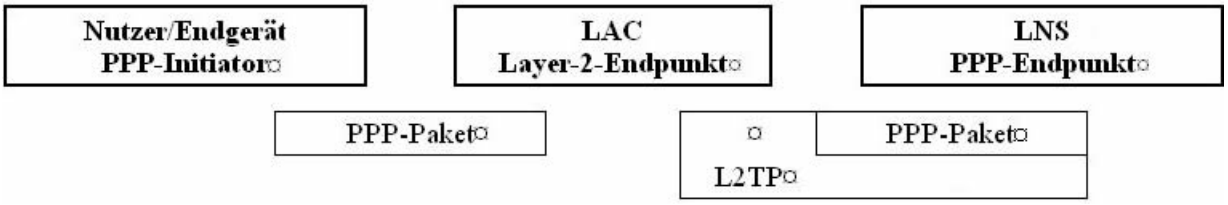


Abbildung 16 L2TP-Tunnel zwischen LAC und LNS

Vom Endgerät werden zu übertragende Nutzdaten, z. B. IP-Pakete, zunächst in PPP verpackt und an den LAC gesendet. Der LAC packt die PPP-Pakete in den vorher aufgebauten L2TP-Tunnel und sendet diese zum LNS an den PPP-Endpunkt. In umgekehrter Richtung werden Nutzdaten am LNS zunächst in PPP und diese in L2TP gepackt und zum LAC gesendet. Dieser entfernt den L2TP-Tunnelrahmen und sendet die PPP-Pakete zum Endgerät weiter.
Die Authentisierung zwischen Nutzer und LNS erfolgt auf PPP-Ebene mittels PAP, CHAP (Challenge Handshake Authentication Protocol) oder anderen Authentisierungsmechanismen außerhalb von L2TP. Die Kommunikation zwischen LAC und LNS auf L2TP-Ebene kann ebenfalls durch Authentisierung mit einem Kennwort abgesichert werden.
Genutzt werden kann das L2TP-Protokoll, um dezentrale Einwahlknoten (LAC) zu betreiben und die Endknoten der Netzverbindungen (LNS) zentral zu halten. Beide Komponenten können in der Hand von Providern sein, es ist aber auch denkbar, dass eine große Organisation von einem Dienstleister dezentrale Einwahlkapazitäten (LAC) anmietet, dabei aber die Netzverbindungen an einem eigenen LNS terminieren lässt.

4.2.1.2 L2TP und IPSec

Interessant im Kontext dieser Studie ist der Fall, dass im Endgerät der LAC integriert ist und gleichzeitig der L2TP-Tunnel mit Hilfe von IPSec kryptographisch gesichert wird. In diesem Fall wird zwischen IPSec-Initiator und IPSec-Endpunkt ein IPSec-Tunnel aufgebaut, in dem wiederum vom LAC zum LNS eine L2TP-Verbindung aufgebaut wird. In diesem L2TP-Tunnel wird dann eine PPP-Verbindung erzeugt (vgl. Abbildung 17).

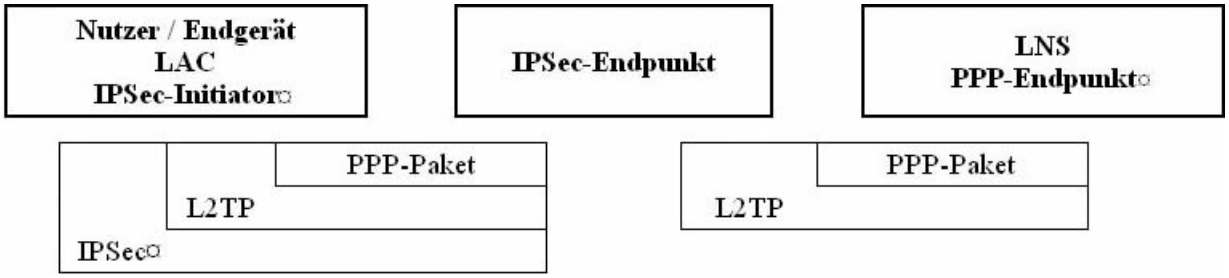


Abbildung 17 PPP/L2TP/IPSec-Tunnel (getrennter LNS)

IPSec-Endpunkt und LNS sind hier als getrennte Geräte symbolisch dargestellt worden. Es besteht die Möglichkeit, beide Komponenten in einem Endgerät zu vereinen. Dann erhält man, was mit „IPSec over L2TP“ üblicherweise gemeint ist (vgl. Abbildung 18).

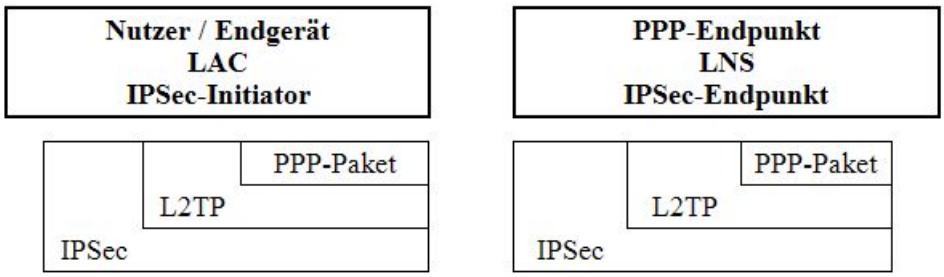


Abbildung 18 PPP/L2TP/IPSec-Tunnel (integrierter LNS)

Folgende Prozesse müssen ablaufen, wenn “PPP über L2TP über IPSec” als VPN-Tunnel genutzt werden soll:

1. Verhandlung und Aufbau eines IPSec-Tunnels
2. Aufbau eines L2TP-Tunnels
3. Aushandlung der PPP-Verbindung im bestehenden IPSec/L2TP-Tunnel

Nutzdaten werden also von einem Tunnelende zunächst in PPP verpackt, diese dann in L2TP, und zum Schluss erfolgt eine Einbettung der L2TP-Pakete in den IPSec-Tunnel. Gelangen die Pakete nach der Versendung an das andere IPSec-Tunnelende, läuft der umgekehrte Prozess ab.

Grundsätzlich kann ein L2TP-Tunnel über ein beliebiges paketvermittelndes Netz aufgespannt werden. Der RFC nennt hier als Beispiele IP, Frame Relay oder ATM. Bis auf IP werden die Transfermechanismen jedoch nicht weiter spezifiziert.

Im Studienkontext wird L2TP ausschließlich im Zusammenhang mit IPSec betrachtet. IPSec kann jedoch naturgemäß nur IP-Verbindungen absichern. Der Einsatz von IPSec erfordert daher zwingend einen über IP aufgebauten L2TP-Tunnel. Diese Beschränkung gilt jedoch nur für den L2TP-Tunnel. Im inneren PPP-Tunnel können nach wie vor beliebige (beispielweise IPX- oder Appletalk-) Pakete übertragen werden.

4.2.1.3 L2TP in UDP

Wenn ein L2TP-Tunnel über eine IP-Strecke aufgebaut wird, wird der UDP-Port 1701 für den Listener genutzt. Dieser Port wird auch für L2F genutzt, die Unterscheidung erfolgt laut RFC 2661 anhand der Versionsnummer im L2TP-Header. Die Quellports sind nicht eingeschränkt.

Der Initiator eines L2TP-Tunnels (LAC oder LNS) wählt als UDP-Quellport einen beliebigen freien Port aus. Er schickt das erste Datenpaket an den Kommunikationspartner mit UDP-Zielport 1701. Die Antwort kann auf einem beliebigen UDP-Quellport erfolgen. Als UDP-Zielport der Antwortpakete wird wie gewöhnlich der vom Initiator urprünglich gewählte Quellport verwendet. Für den gesamten Lebenslauf des L2TP-Tunnels bleiben danach die gewählten Ports auf beiden Seiten gleich.

Jedes einzelne L2TP-Datenpaket wird immer in einem einzigen UDP-Datagramm übertragen. Ist das Datagramm zu groß für die IP-Übermittlungsstrecke, ist daher mit Fragmentierung zu rechnen. L2TP hat keine eingebauten Mechanismen, um Fragmentierung zu verhindern – der RFC 2661 schlägt lediglich vor, auf PPP-Ebene am LAC mit dem Link Control Protocol (LCP) die Maximum Transmission Unit (MTU) mit Rücksicht auf die Übertragungsstrecken passend auszuhandeln.

4.2.1.4 Struktur von L2TP-Nachrichten

Ein L2TP-Paket weist folgenden Aufbau auf:

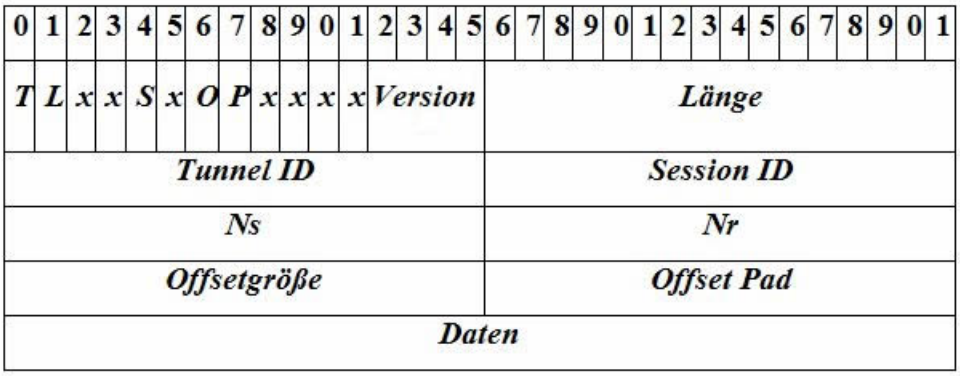


Abbildung 19 Struktur von L2TP-Nachrichten

Bezeichnung	Erläuterung
T	Zeigt an, ob diese Nachricht eine Daten- (T = 0) oder eine Steuernachricht (T = 1) ist.
L	Falls gesetzt, gibt es das Feld Länge in der Nachricht.
x	reserviert für künftige Erweiterungen
S	Falls gesetzt, gibt es die Felder Ns und Nr in der Nachricht.
O	Offset Falls gesetzt, gibt es das Feld Offsetgröße in der Nachricht.
P	Priorität Falls in Datennachrichten gesetzt, sollte die Nachricht in Warteschlangen und bei der Weiterverarbeitung bevorzugt behandelt werden. Steuernachrichten müssen hier ein gelöschtes Bit vorweisen.
Version	Enthält die L2TP-Protokollversion und muss auf den Wert 2 gesetzt werden. Der Wert 1 ist reserviert, um ein L2F-Paket zu detektieren, falls dieses vermischt mit L2TP-Paketen ankommt. Eingehende Pakete mit einem anderen, unbekannten Wert müssen gelöscht werden.
Länge	Gesamtlänge der Nachricht in Bytes. Existiert in jeder Steuernachricht, in Datennachrichten aber nur, falls das L-Bit gesetzt ist.
Tunnel ID	Identifikator für die Steuerverbindung. L2TP-Tunnel werden mit Identifikatoren benannt, die lediglich eine lokale Signifikanz haben. Daher wird derselbe Tunnel unterschiedliche Tunnel-IDs an jedem Tunnelende aufweisen, wobei die Tunnel-ID in der Nachricht die ID des Empfängers ist. Tunnel-IDs werden während der Tunnelaufbauphase generiert und als Assigned-Tunnel-ID Attribut-Wert-Paare ausgetauscht.
Session ID	Session ID (16 Bits) Identifikator für eine Session innerhalb eines Tunnels. L2TP-Sessions werden mit Identifikatoren benannt, die lediglich eine lokale Signifikanz haben. Daher wird dieselbe Session unterschiedliche Session-IDs an jedem Session-Ende aufweisen, wobei die Session-ID in einer übermittelten L2TP-Nachricht die ID des Empfängers ist. Session-IDs werden während der Sessionaufbauphase generiert und als Assigned-Session-ID Attribut-Wert-Paare ausgetauscht.
Ns	Zeigt die Sequenznummer für diese Daten- oder Steuernachricht an.

Nr	Zeigt die Sequenznummer an, die in der nächsten zu empfangenden Steuernachricht erwartet wird
Offsetgröße	Größe des Feldes Offset Pad, Anzahl der Bytes hinter dem L2TP-Header und vor dem Beginn der Nutzdaten. Ist nur in Datennachrichten vorhanden, und dort auch nur, wenn das Feld O dies anzeigt. Falls das Feld Offsetgröße vorhanden ist, endet der L2TP-Header nach dem letzten Byte des Offset Pad.
Offset Pad	Ist nur in Datennachrichten vorhanden und dort auch nur, wenn das Feld O dies anzeigt. Die Länge dieses Feldes steht dann im Feld Offsetgröße. Tatsächlich gesendete Daten innerhalb des Offset Pad gelten als undefiniert.
Daten	Hier befinden sich die eigentlichen Nutzdaten (PPP-Pakete oder L2TP-Steuerinformationen).

4.2.1.5 Kommunikationsauf- und -abbau

Für eine L2TP-Verbindung werden zwei logische Kanäle benötigt:

- L2TP-Datenkanal
  In diesem Kanal werden die Nutzdaten zwischen LAC und LNS übertragen. Hierbei handelt es sich um in L2TP-Datenpaketen eingepackte PPP-Frames. Verlorengegangene Datenpakete werden nicht erneut übertragen.
- L2TP-Steuerkanal
  Hier werden ausschließlich Steuer- und Kontrollnachrichten zwischen LAC und LNS ausgetauscht. Der Verlust von Steuerpaketen wird erkannt, und verlorene Pakete werden erneut übertragen.

Wenn der L2TP-Tunnelaufbau durch Authentisierung abgesichert werden soll, wird beim Tunnelaufbau per CHAP zwischen LAC und LNS die Kenntnis des Kennworts (Shared Secret) verifiziert.

L2TP ist ein zustandsorientiertes Protokoll: Beide beteiligten L2TP-Partner (LAC und LNS) kennen zu jeder Zeit den Zustand der L2TP-Session.

Ein typischer Verbindungsaufbau eines L2TP-Steruerkanals sieht dabei wie folgt aus:

- SCCRQ (Start-Control-Connection-Request)
  Der L2TP-Initiator (LAC) sendet dem LNS einen Start-Control-Connection-Request. Dieser Request initiiert den Aufbau eines Steuerkanals. Er enthält eine Reihe von Attribut-Wert-Paaren, die zum Aufbau der Verbindung und zur Aushandlung von Tunnelparametern dienen.
- SCCRP (Start-Control-Connection-Reply)
  Der LNS antwortet mit einem Start-Control-Connection-Reply. Damit wird dem Initiator zum einen der Empfang des SCCRQ signalisiert. Zum anderen werden die Tunnelparameter (Attribut-Werte-Paare), die der LNS im SCCRQ erhalten hat, aus der Sicht des LNS an den LAC kommuniziert.
- SCCCN (Start-Control-Connection-Connected)
  Der LAC antwortet wiederum mit einem Start-Control-Connection-Connected. Damit wird dem LNS im Wesentlichen der Empfang des SCCRP signalisiert.
- ZLB (Zero-Length-Bit-Message)
  Vom LNS an den LAC: Zero-Length-Bit-Message, eine Bestätigung zum Paketempfang.

Der Tunnel könnte auch in umgekehrter Richtung aufgebaut werden, dann würden sich hier die Rollen von LAC und LNS vertauschen.

Innerhalb eines L2TP-Tunnels besteht die Möglichkeit, einen Keepalive-Mechanismus durch den Austausch von „Hello“-Nachrichten zu etablieren. Diese Nachrichten können von beiden Partnern generiert werden.

Ein L2TP-Datenkanal wird typischerweise über die folgende Sequenz im L2TP-Steuerkanal aufgebaut:

- ICRQ (Incoming-Call-Request)
  Der LAC schickt einen Incoming-Call-Request. Damit wird dem LNS ein am LAC eingehender Ruf signalisiert.
- ICRP (Incoming-Call-Reply)
  Der LNS bestätigt mit einem Incoming-Call-Reply.
- ICCN (Incoming-Call-Connected)
  Der LAC bestätigt mit einem Incoming-Call-Connected.
- ZLB (Zero-Length-Bit-Message)
  Vom LNS an den LAC: Zero-Length-Bit-Message, eine Bestätigung zum Paketempfang.

Damit ist auch der L2TP-Datenkanal aufgebaut, und jetzt erst kann der PPP-Kanal aufgebaut werden. Eine PPP-Sitzung erfordert zwingend einen vorherigen vollständigen Aufbau eines L2TP-Tunnels, d. h. den Aufbau eines Datenkanals mit genau einer Session pro PPP-Call sowie eines L2TP-Steuerkanals. Jede PPP-Verbindung wird in einer eigenen Session geführt. Dabei ist es aber erlaubt, mehrere L2TP-Sessions in einem L2TP-Tunnel zu führen und ebenso mehrere Tunnel zwischen einem LAC-LNS-Paar.

Der PPP-Verbindungsaufbau geschieht wie in RFC 1661 ausgeführt durch den Austausch von LCP- (Line Control Protocol) und anschließend (bei IP) von IPCP (IP Control Protocol)-Paketen. Danach werden alle PPP-Pakete in L2TP-Frames eingebettet.

Wenn der PPP-Kanal durch LCP-Steuerpakete wieder abgebaut worden ist, kann auch der L2TP-Datenkanal durch die folgenden Befehle wieder abgebaut werden:

- CDN (Call-Disconnect-Notification)
  Der LAC signalisiert eine Call-Disconnect-Notification.
- ZLB (Zero-Length-Bit-Message)
  Vom LNS an den LAC: Zero-Length-Bit-Message, eine Bestätigung zum Paketempfang.

Der Abbau des Steuerkanals selbst würde typischerweise nach dem folgenden Schema ablaufen:

- StopCCN (Stop-Control-Connection-Notification)
  Der LAC sendet eine Stop-Control-Connection-Notification.
- ZLB (Zero-Length-Bit-Message)
  Vom LNS an den LAC: Zero-Length-Bit-Message, eine Bestätigung zum Paketempfang.

Der Steuerkanal könnte auch in umgekehrter Richtung abgebaut werden, dann würden sich hier die Rollen von LAC und LNS vertauschen.

Abbildung 20 zeigt den typischen Verbindungsauf- und -abbau in grafischer Form.

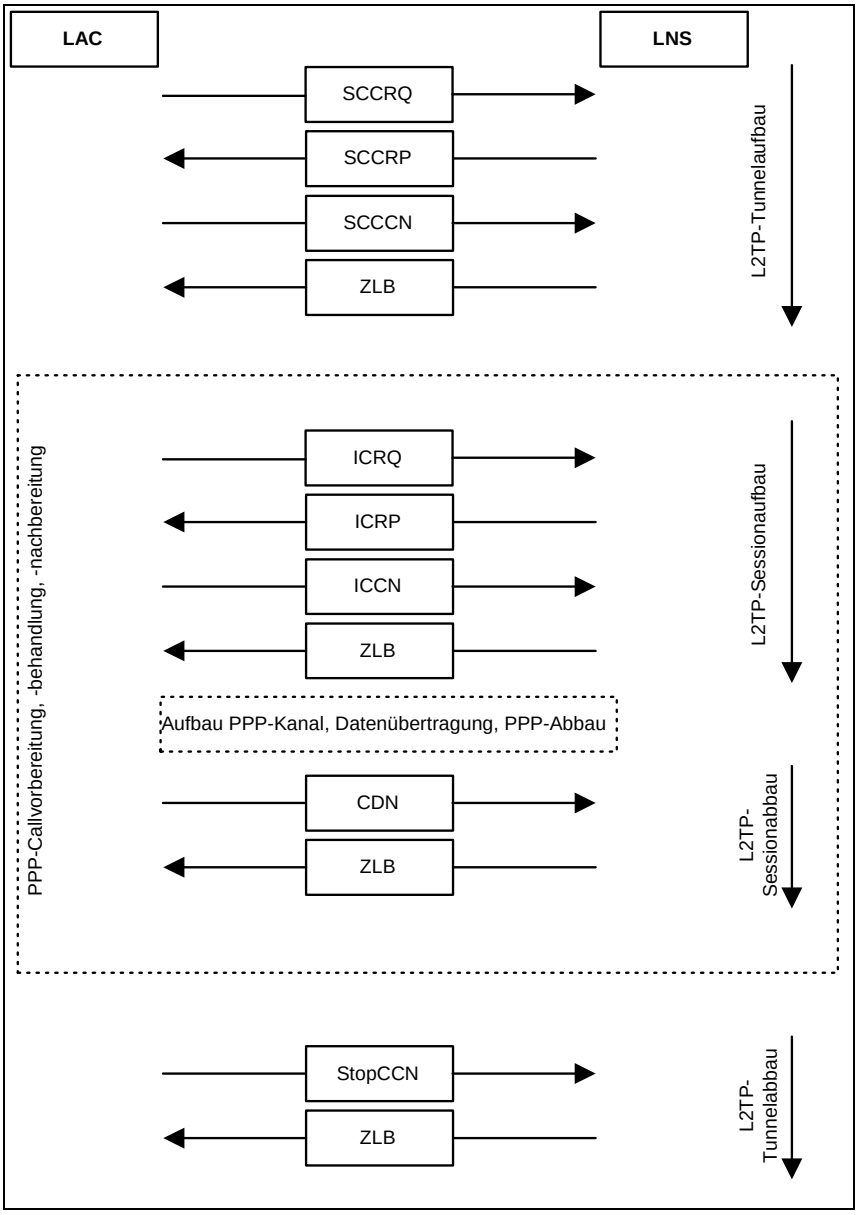


Abbildung 20 L2TP-Verbindungsauf- und -abbau

Die innere Ablauflogik, d. h. der L2TP-Sessionauf- und -abbau als Behandlung eines PPP-Calls, erfolgt pro PPP-Call. Die äußere Ablauflogik, d. h. der L2TP-Tunnelauf- und –abbau, muss nicht pro PPP-Call ablaufen, der Tunnel kann persistent sein.

4.2.2 Einordnung im ISO-Schichtenmodell

L2TP wird als UDP-Protokoll implementiert, und die L2TP-Pakete werden innerhalb der Sitzungsschicht – meist auf Basis von IP – transferiert.

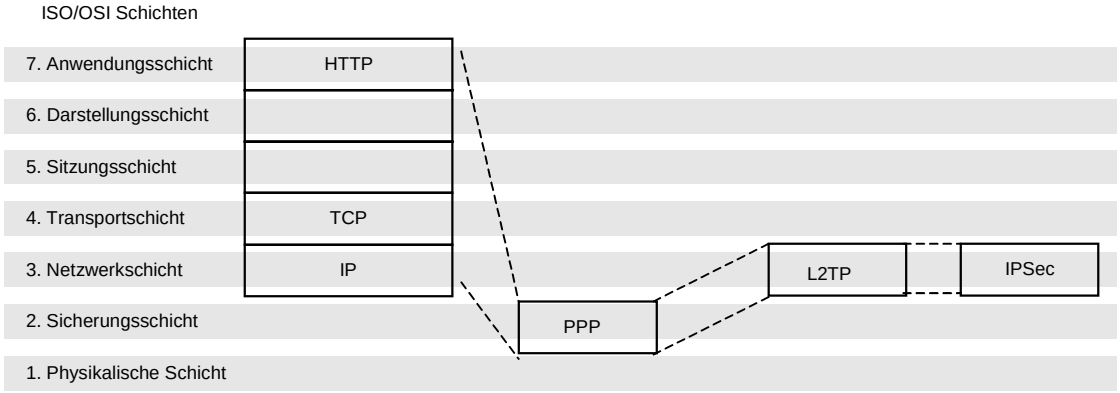


Abbildung 21 IPSec/L2TP/PPP im ISO/OSI-Schichtenmodell

4.2.3 Benötigte Paketfilterregeln

Sofern sowohl der IPSec- als auch der L2TP-Tunnel am gleichen Endgerät terminieren, verläuft die abzusichernde Kommunikation auf IPSec-Ebene. Die Paketfilterregeln bei der Filterung von IPSec/L2TP/PPP gleichen somit denen einer IPSec-Filterung. Diese wurden bereits in Kapitel 4.1.7 vorgestellt.

4.2.4 Integration in Sicherheitsgateways

Im Prinzip könnte man die Kombination aus L2TP und IPSec bei der Integration in Sicherheitsgateways wieder trennen und auf unterschiedlichen Geräten implementieren. Die folgende Abbildung zeigt diese Architektur schematisch:

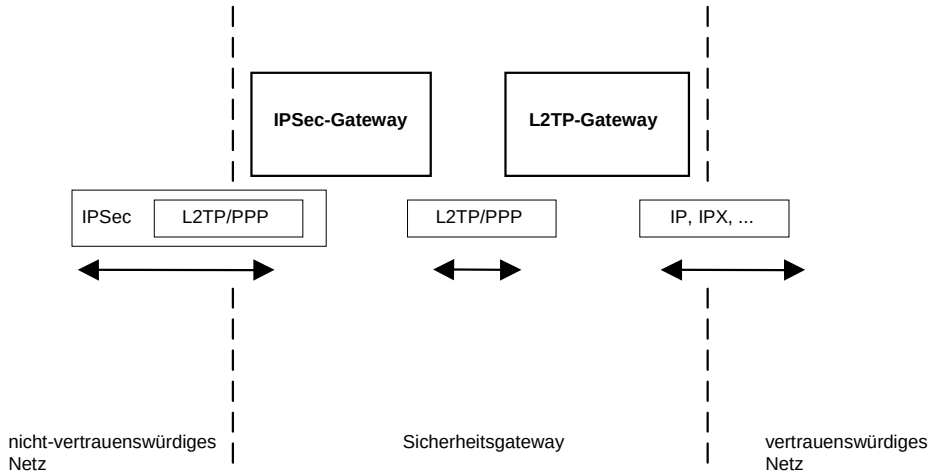


Abbildung 22 Integration in Sicherheitsgateways

Am IPSec-Gateway terminiert der IPSec-Tunnel, während der L2TP/PPP-Tunnel weiter innen am L2TP-Gateway terminiert. Bis auf wenige Sonderfälle dürfte diese architektonische Trennung beider Tunnel jedoch keinerlei Sicherheitsgewinn erbringen. Darüber hinaus wird diese Architektur von dem am weitesten verbreiteten L2TP-Gerät (Microsoft L2TP-Client) nicht unterstützt, weil IPSec im Microsoft-Stack nur den Transport-Mode beherrscht, während in der hier gezeigten Architektur IPSec im Tunnel-Mode erforderlich wäre. Daher wird diese Architektur hier nicht weiter behandelt.

Verzichtet man auf die konzeptionelle Trennung von IPSec- und L2TP/PPP-Tunnelendpunkt und lässt man den geschachtelten Tunnel statt dessen in einem einzigen Endpunkt terminieren, können die Paketfilterregeln aus Kapitel 4.1.7 verwendet werden.

4.2.5 Umgang mit Network Address Translation (NAT)

Bei der Verschlüsselung von L2TP mittels IPSec gibt es gegenüber anderen IPSec-Verschlüsselungen (s. Abschnitt 4.1.5) grundsätzlich keinerlei Besonderheiten hinsichtlich der NAT-Problematik.

Ein L2TP-Tunnel kann grundsätzlich mit IPSec sowohl im Tunnel- als auch im Transport-Mode aufgebaut werden. RFC 3193 spezifiziert den Einsatz von L2TP im IPSec-Kontext genauer und fordert, dass L2TP/IPSec-Implementierungen den IPSec-Transport-Mode unterstützen müssen – der Tunnel-Mode ist jedoch nur optional. In der Praxis findet man daher vorwiegend IPSec/L2TP-Implementierungen, die ausschließlich den Transport-Mode beherrschen.

Der im NAT-Kontext problematische Transportmodus (s. Abschnitt 4.1.5) wird somit als verbindliche Implementationsvorgabe festgelegt. IPSec-Pakete im Transportmodus können kryptographisch geschützte TCP-/UDP-Checksummen enthalten, die von einem NAT-Gerät bei einer Änderung des IP-Headers nicht angepasst werden können.

Das Problem könnte wie folgt umgangen werden: Bei UDP ist im Gegensatz zu TCP eine Checksummenbildung nicht obligatorisch, sondern erlaubt ist auch, im UDP-Prüfsummenfeld eine 0 abzulegen. Wenn also beide L2TP-Tunnelendpunkte keine UDP-Checksummen erzeugen würden, wäre eine IPSec-Verbindung auch im IPSec-Transport-Mode möglich. Es existieren jedoch keine Produkte, die entsprechende Checksummen erzeugen.

Bei einem NAT-Gerät zwischen den Tunnelenden ist somit ein IPSec/L2TP/PPP-Tunnel nur dann erfolgreich zu betreiben, wenn beide Partner NAT-fähig sind

4.2.6 Checkliste Sichere Konfiguration

Die Checkliste hinsichtlich einer sicheren Konfiguration von IPSec/L2TP unterscheidet sich nicht von der Checkliste für einen reinen IPSec-Tunnel (vgl. Kapitel 4.1.8). L2TP selbst bietet – bis auf die Möglichkeit, den L2TP-Tunnel durch Kennwortschutz auf Benutzerebene zu authentisieren – keine Sicherheitsfunktionen.

4.2.7 Häufig auftretende Probleme

Der Konfigurationsaufwand bei vielen L2TP/PPP-Implementierungen ist gering. IP-Adresse, DNS- und ggf. WINS-Serveradressen (“Windows Internet Naming Service”) werden dem Client auf PPP-Ebene für den Zeitraum der Verbindung zugeordnet. Auf L2TP-Ebene wird in der Praxis die Authentisierungsfunktion nicht genutzt: Die Authentisierung wird bereits am äußeren IPSec-Tunnel und im inneren PPP-Tunnel durchgeführt, so dass eine dritte, maschinenspezifische Authentisierung im L2TP-Tunnel keinen Sicherheitsgewinn bedeutet.

Probleme ergeben sich fast ausschließlich aus der Verwendung von IPSec zur Sicherung der Daten. Hier unterscheiden sich die Probleme aber nicht von denen eines reinen IPSec-Tunnels, die in Kapitel 4.1 behandelt wurden.

Die Problematik bzgl. des NAT-Traversals behandelt Abschnitt 4.1.5.

4.3 Secure Socket Layer (SSL)/Transport Layer Security (TLS)

Secure Socket Layer (SSL) wurde in den frühen 90er Jahren von der Firma Netscape entwickelt, um für das ungesicherte HTTP-Protokoll Sicherheitsmechanismen bereitzustellen. SSL bietet Mechanismen zur Authentifizierung, zur Verschlüsselung und zur Integritätssicherung einer Kommunikationsverbindung. Es unterstützt die Verwendung von Zertifikaten, optional beidseitig einer SSL-Verbindung, kann aber auch mit einfachen Authentisierungsmethoden, z. B. mittels Benutzername und Passwort, abgesichert werden.

Obwohl der Einsatz im HTTP-Umfeld die eigentliche Motivation für die Spezifikation von SSL war, wurde SSL in allen veröffentlichten Versionen anwendungsunabhängig spezifiziert, es ist also in der Lage, prinzipiell jede TCP-Anwendungskommunikation mit Kryptomechanismen abzusichern.

SSL kann bzgl. der Sicherheit in der Regel feiner abgestimmt werden als andere VPN-Technologien, da wesentlich mehr Parameter zur Konfiguration zur Verfügung stehen. SSL kann ebenfalls verwendet werden, um einzelne Dienste über VPN bereitzustellen, bei anderen VPN-Technologien wird oft ein ganzer Server mit allen von diesem angebotenen Diensten zur Verfügung gestellt, falls nicht weitere Sicherheitskomponeten eingesetzt werden, wie z. B. ein Paketfilter.

Die Unterschiede zwischen Transport Layer Security (TLS) und SSL sind marginal, z. B. gibt es bei TLS mehr Alert-Nachrichten als bei SSL Version 3 (SSLv3), und es gibt bei Blockverschlüsselungsmethoden die Möglichkeit des Block-Paddings.

SSLv3 hat sich flächendeckend durchgesetzt und SSLv2 verdrängt. Wenn im Folgenden von SSL die Rede ist, ist damit SSLv3 gemeint.

4.3.1 Einordnung im ISO-Schichtenmodell

SSL ist ein anwendungsunabhängiges Protokoll. Es ist im IP-Stack oberhalb der Transportschicht (“TCP-Schicht”) anzusiedeln (vgl. Abbildung 23).

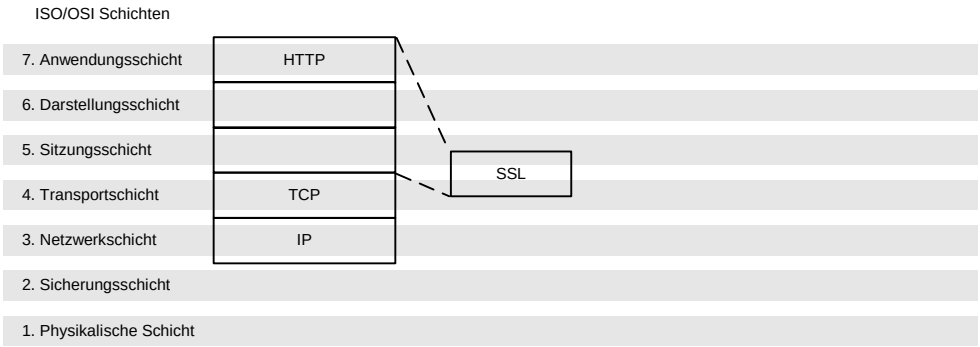


Abbildung 23 SSL im ISO/OSI-Schichtenmodell

4.3.2 Kommunikationsauf- und -abbau

Bei einer SSL-/TLS-Verbindung erfolgt der Kommunikationsaufbau wie in Abbildung 24 skizziert. Diese Aufbausequenz kann variieren, abhängig davon, ob ein Client-Zertifikat verwendet wird und ob ein geeignetes Server-Zertifikat vorhanden ist. Außerdem können unter bestimmten Randbedingungen zusätzliche Schritte beim Schlüsselaustausch notwendig sein.

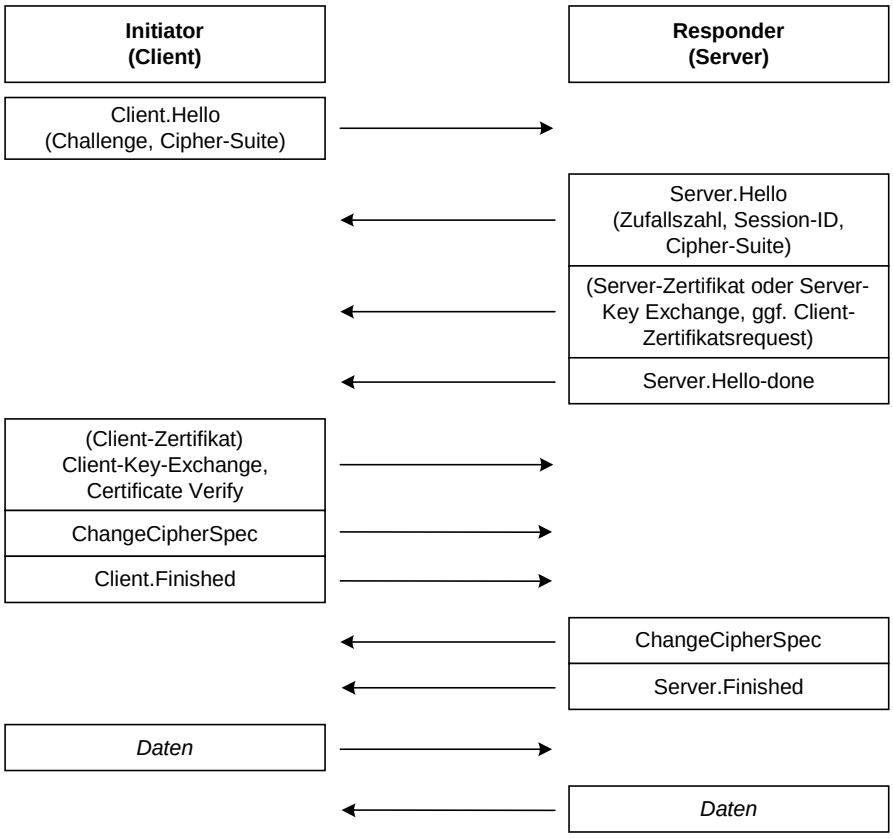


Abbildung 24 Kommunikationsaufbau einer SSL Sitzung

Der Client beginnt und sendet eine Client.Hello-Nachricht an den Server. Sie enthält folgende Informationen:

- die vom Client erwünschte SSL-Versionsnummer. Falls der Client SSLv2 und SSLv3 unterstützt, wird er die Client.Hello-Nachricht im SSLv2-Format senden, aber als erwünschte Versionsnummer 3.0 anfordern;
- die aktuelle Zeit;
- (optional) eine Session-ID. Falls die Session-ID fehlt, wird der Server versuchen, eine unterbrochene Sitzung wieder aufzunehmen. Kann er das nicht, generiert er eine neue Session-ID;
- die vom Client unterstütze Cipher-Suite (Liste der unterstützten Authentifizierungmodi, Schlüsselaustauschmethoden, Verschlüsselungs- und MAC-Algorithmen);
- die vom Client unterstützten Kompressionsmethoden;
- eine Zufallszahl;

Der Server evaluiert die Client.Hello-Nachricht und antwortet mit einer Server.Hello-Nachricht. Sie enthält folgende Informationen:

- die vom Server erwünschte SSL-Versionsnummer;
- die aktuelle Zeit;
- die Session-ID;
- die vom Server aus der Vorschlagsliste des Clients ausgewählte Cipher-Suite;
- die vom Server unterstützten Kompressionsmethoden;
- eine Zufallszahl;

Im Anschluss an die Server.Hello-Nachricht wird der Server sein Zertifikat verschicken. Falls er keines besitzt oder sein Zertifikat nur zum Signieren zugelassen ist, sendet er statt des Zertifikats eine „Server-

Key-Exchange“-Nachricht. Es folgt ggf. eine Aufforderung an den Client, seinerseits dessen Zertifikat zu übermitteln.

Der Server schließt seine Nachricht mit Server.Hello-done.

Der Client evaluiert die Server.Hello-Nachricht und antwortet mit folgenden Informationen:

- Falls angefordert, das Client-Zertifikat. Wenn er über kein Client-Zertifikat verfügt, aber eines angefordert wurde, sendet er eine No-Certificate-Nachricht.
- Falls der Server eine „Server-Key-Exchange“-Nachricht gesendet hatte, antwortet der Client mit einer „Client-Key-Exchange“-Nachricht auf der Basis des Public Key Algorithmus in der Cipher-Suite aus den Hello-Nachrichten.
- Falls der Client ein Zertifikat gesendet hat, verifiziert der Client das Server-Zertifikat und sendet eine Zertifikats-Verifikationsnachricht mit dem Prüfergebnis.

Im Anschluss daran versendet der Client eine ChangeCipherSpecs-Nachricht und signalisiert anschließend mit einer Finished-Nachricht das Ende des Handshakes (ChangeCipherSpec ist, streng genommen, ein unabhängiger Content Type und keine Handshake-Nachricht).

Der Server antwortet mit einer Kombination aus ChangeCipherSpec und Finished. Die Finished-Nachricht des Servers ist die erste verschlüsselte Nachricht.

Während der letzten Phase des Handshakes generieren beide Session-Partner aus dem ausgetauschten Material einen Encryption Key. Danach kann der Austausch der Daten auf Anwendungsebene in gesicherter Weise erfolgen.

Wird eine unterbrochene Session wieder aufgenommen oder zu einer bestehenden Session eine weitere parallele aufgebaut, wird nicht der gesamte Initialisierungszyklus durchlaufen. Insbesondere werden nicht erneut Zertifikate ausgetauscht. Vielmehr wird die wiederaufgenommene oder zusätzliche Session mit Hilfe der noch bestehenden Session aufgebaut. Die Referenz auf eine noch bestehende Session erfolgt dabei mit Hilfe der Session-ID, die für eine gewisse Lebensdauer im Server-Cache verbleibt. Bei einer zusätzlichen Session werden jedoch immer auch ChangeCipherSpec-Nachrichten zum Schluss der Initialisierungsphase übermittelt.

Die Kommunikation wird durch eine spezielle Alert-Nachricht (close_notify) von einer der beteiligten Sitzungspartner beendet. Der andere Partner sollte danach mit einem gleichen Alert (close_notify) antworten. Alle danach noch gesendeten Daten, die sich auf diese SSL-Sitzung beziehen, werden ignoriert.

4.3.3 Verschlüsselung und Paketstruktur

SSL-Nachrichten werden in Records übermittelt. In SSLv3 und TLS sind diese Records wie folgt aufgebaut:

Content Type	Version	Länge	(Nutz-)Daten

Abbildung 25 SSL-Recordstruktur

Der Record-Header, bestehend aus Content-Typ, Versionsnummer und Längenangabe, wird nicht verschlüsselt.

Als Content-Typ sind momentan Application, Handshake, Alert und Change Cipher spezifiziert:

- Typ Alert teilt dem Gegenüber nicht akzeptierte Parameter beim Verbindungsaufbau, unerwartete Nachrichten, Fehler oder das Ende einer SSL-Sitzung mit.

- Typ Handshake dient zum Aushandeln von Verbindungs- und Sitzungsparametern.
- Mit ChangeCipherSpec-Nachrichten werden kryptographische Parameter für die aufzubauende oder bestehende Sitzung ausgehandelt und mitgeteilt.
- Typ Application enthält die Informationen der Anwendung, die SSL nutzt.

Man beachte, dass man im Klartext-Teil lediglich den Content-Typ, die SSL-Version und die Länge des folgenden Nutzdatenblocks erkennen kann, nicht jedoch den verschlüsselten Inhalt. Man kann also beispielsweise ohne Kenntnis des Sitzungsschlüssels erkennen, ob eine SSL-Nachricht ein Alert übermittelt, aber nicht, um welchen Alert es sich handelt.

Als Schlüsselaustauschmethoden sind Fortezza, RSA und Diffie-Hellman verfügbar. Fortezza ist in TLS formal nicht mehr in einer Cipher-Suite enthalten. Allerdings werden die noch in SSLv3 dafür definierten Flags im TLS-Standard ausdrücklich als „reserved“ deklariert. RSA kommt vorwiegend zum Einsatz, wenn Zertifikate verwendet werden. Ansonsten wird der Schlüsselaustausch gemäß Diffie-Hellman vollzogen. Sowohl die RSA- als auch die Diffie-Hellman-Methode kann auf 512 Bit Schlüssellänge eingeschränkt sein – die Verwendung derart kurzer Schlüssel sollte aber unter allen möglichen Umständen vermieden werden.

Die Integrität der Nachrichten wird entweder mit MD5 oder SHA-1 abgesichert. Beide Methoden sind als vergleichbar sicher einzustufen.

4.3.4 SSL-VPN-Ausprägungen

SSL-VPN ist ein Sammelbegriff für die verschiedenen Techniken, die basierend auf SSL ein VPN erzeugen können. Die Einsatzszenarien reichen von einer sicheren Anbindung an ein Web-Portal über die Tunnelung von einzelnen Diensten bis hin zur vollwertigen Anbindung (=Bereitstellung aller auf IP basierenden Dienste) an ein Subnet. Diese sehr unterschiedlichen Techniken werden im Folgenden anhand von grafischen Darstellungen kategorisiert und erläutert.

4.3.4.1 Zentrales Web-Portal als generischer SSL-Proxy

Um einem externen Client Zugang zu Teilen der internen Infrastruktur zu ermöglichen, können im einfachsten Fall bereits bestehende interne Web-Infrastrukturen unter Zuhilfenahme eines benutzerspezifisch geschützten Zugangs SSL-fähig gemacht werden. Am Client reicht dazu ein beliebiger SSL-fähiger Browser und als entgegengesetzter Endpunkt ein spezieller SSL-Proxy aus.

In diesem Fall wird dem externen Nutzer nach der Authentisierung vom SSL-Proxy eine benutzerspezifische Web-Eingangsseite geboten. Auf der Web-Seite sind Hyperlinks vorhanden, bei deren Betätigung der zentrale SSL-Proxy die Zugriffe auf die eigentlichen Web-Seiten durchführt und den Datenstrom durch den bestehenden SSL-Tunnel zum Client sendet.

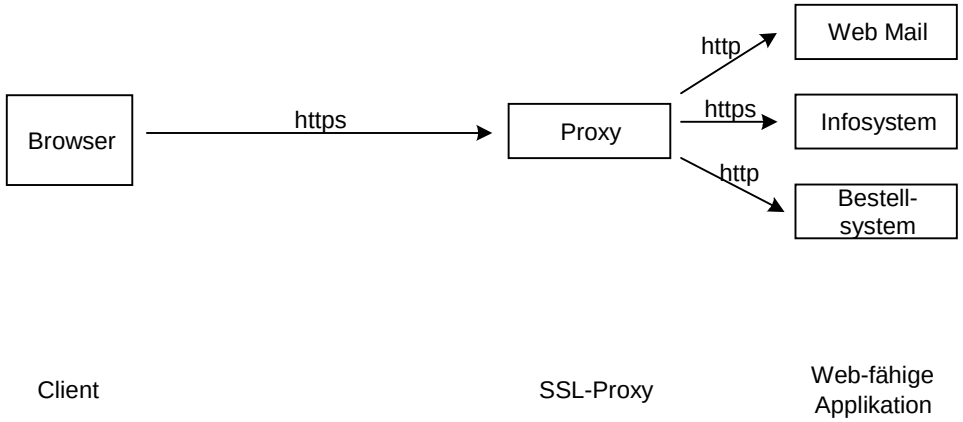


Abbildung 26 Zentrales Web-Portal als SSL-Proxy

Beispiele dafür könnten der firmenintern bestehende Mail-Zugang sein, der bereits von Hause aus über eine Web-Schnittstelle verfügt, oder auch jeder andere bereits bestehende interne Web-Dienst, also z. B. Bestellsysteme oder Informationssysteme. Der Mehrwert des zentralen SSL-Proxies besteht in der Bereitstellung von Authentisierungs- und Autorisierungsfunktionen sowie Integritäts- und Vertraulichkeitsschutz.

4.3.4.2 Zentraler SSL-Proxy mit „Webbifizierungs-Funktion“

Eine Kapselung in HTTPS kann verwendet werden, wenn externen Clients interne Dienste angeboten werden sollen, die von sich aus keine Web-Unterstützung bieten. Beispiele dafür sind Fileservices wie das Network File System (NFS): Der Zugang zu internen Fileservices wird hier vom SSL-Proxy über eine Web-Seite mit speziellen Hyperlinks geboten. Der SSL-Proxy wird dadurch gleichzeitig zu einem Web-Server. Wird ein Link ausgewählt, muss der SSL-Proxy im Namen des Clients mittels NFS auf den gewünschten Fileserver zugreifen, die Anwort des Fileservers in HTML umsetzen und durch den bestehenden SSL-Kanal mittels HTTP zum Browser senden.

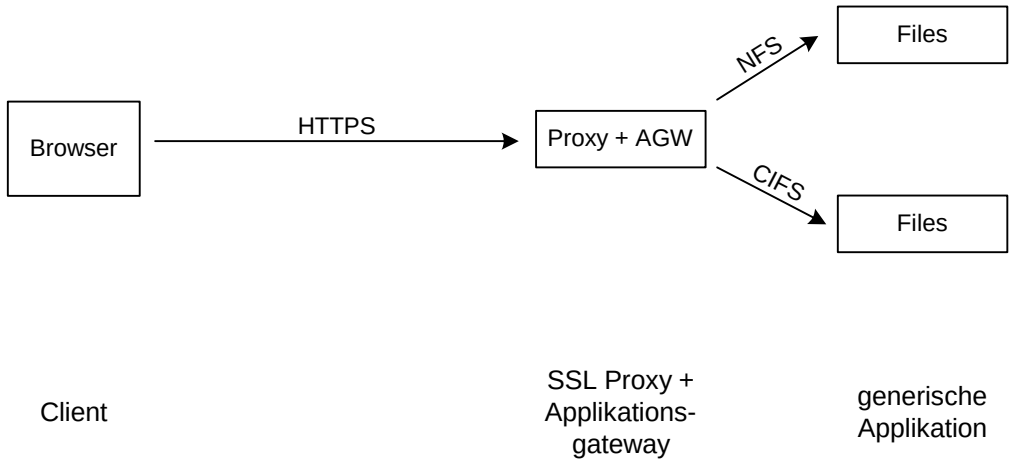


Abbildung 27 Zentraler SSL-Proxy mit Webbifizierungs-Funktion

Die beschriebene Umsetzung von Anwendungsprotokollen in HTTP/HTML wird häufig als „Webbifizierung“ bezeichnet. Diese Vorgehensweise erfordert spezielle Fähigkeiten des zentralen

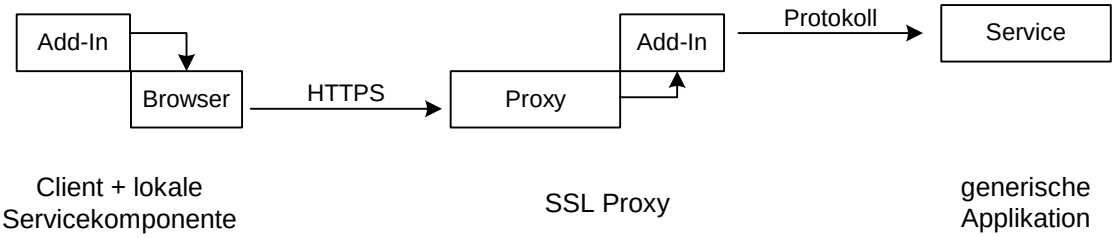
Proxies und wird in der Regel wegen des hohen Aufwandes nur für eine kleine Anzahl von Anwendungsdiensten implementiert. Am Client reicht hingegen ein beliebiger SSL-fähiger Browser aus.

Das zentrale Web-Portal muss neben der Webbifizierungs-Funktion auch Authentisierungs- und Autorisierungsfunktionen sowie Integritäts- und Vertraulichkeitsschutz bereitstellen.

4.3.4.3 Zentraler SSL-Proxy als Web-Portal und Browsererweiterungen

Alle bislang beschriebenen Varianten benötigen als Client-Software nur einen Browser. Bei den folgenden Varianten muss eine dedizierte Software auf dem Client installiert werden.

Werden SSL-Proxies auf dem Client eingesetzt, können beinahe alle auf TCP basierenden Anwendungsprotokolle durch SSL/TLS getunnelt werden. Dazu muss eine Software – meist mit Java-Applets oder ActiveX-Komponenten realisiert – installiert werden, die am Client eingehende Datenverbindungen durch einen SSL-Tunnel leitet. Tunnelende ist neben dem Client der zentrale SSL-Proxy, der die Nutzdaten aus dem Tunnel entpackt und an das eigentliche Zielsystem weiterleitet:



Ein Beispiele für eine derartige Browser-Integration ist der Fernzugriff mittels Terminal-Servern.

Die Nutzung von aktiven Inhalten innerhalb eines Browsers ist problematisch, weil sie mit Sicherheitsrisiken verbunden ist. Die Installation derartiger Komponenten erfordert darüber hinaus vielfach privilegierte Systemberechtigungen. Die Lösung ist nicht plattformunabhängig und nicht auf jedem System einsetzbar, z. B. einem Web-Terminal am Flughafen.

Das zentrale Web-Portal muss neben der Verteilung der Datenströme an die richtigen Zielsysteme auch Authentisierungs- und Autorisierungsfunktionen sowie Integritäts- und Vertraulichkeitsschutz bereitstellen.

4.3.4.4 Zentraler SSL-Proxy als Web-Portal und Nutzung von Standardapplikationen

Die hier beschriebene Variante entfernt sich völlig vom Browser-Ansatz: Es wird auf dem Client ein SSL-forwarder installiert und so vorkonfiguriert, dass die aus einer Applikation eingehenden Daten über einen SSL-Tunnel an den SSL-Proxy weitergeleitet werden:

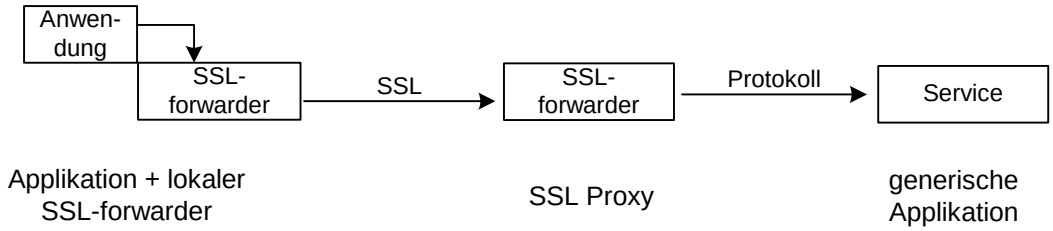


Abbildung 28 Zentrales Web-Portal als SSL-Proxy mit Clientsoftware

Die Anwendungssoftware wird so konfiguriert, dass sie sich beim Start mit dem lokal installierten SSL-forwarder verbindet. Dieser ermittelt aus der Konfigurationsdatei, zu welchem Server über welchen Port er einen SSL-Tunnel aufzumachen und die von der Anwendung erhaltenen Daten zu verschicken hat. Am zentralen Proxy werden die Daten entpackt und zur eigentlichen Nutzanwendung gesendet.

Diese Variante erfordert im Unterschied zur vorhergehenden Variante pro Verbindung, also pro Zielserver und Applikation, einen Tunnel.

Eine Implementation dieser Forwarding-Technik ist „stunnel“.

4.3.4.5 SSL-Tunnel

Wenn man statt einer Applikation einen Netztunnel durch den SSL-Kanal leitet, erhält man eine vollwertige, für viele Anwendungen nutzbare Anbindung in ein Netz. Beim Aufbau eines PPP-Tunnels durch den SSL-Tunnel beispielsweise erhält man eine neue virtuelle Netzschnittstelle, die die Verbindung zwischen den Netzen aufrecht hält.

Dazu wird entweder eine spezielle PPP-Implementierung benötigt, weil diese Implementierung auf eine TCP-Verbindung aufbauen muss. In diesem Fall reicht ein generischer SSL-forwarder aus. Alternativ kann man eine generische PPP-Implementierung dann nutzen, wenn der SSL-forwarder ein für PPP geeignetes Dial-Out-Device emuliert.

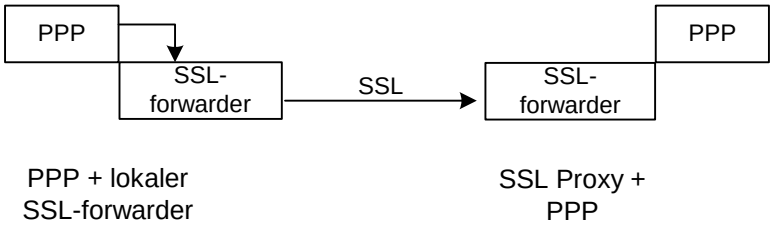


Abbildung 29 SSL-Tunnel

Nachteil dieser Variante sind der zusätzlich aufzubauende PPP-Tunnel und die damit verbundene Verschlechterung der tatsächlich für Anwendungen zur Verfügung stehenden Übertragungskapazitäten zwischen dem Client und dem internen Netz.

Vorteil dieser Variante ist eine vollständige Integration des Clients in das interne Netz. Bei bestehendem Tunnel steht eine generische Netzschnittstelle wie bei normalen Dial-In-Verbindungen zur Verfügung. Diese Netzschnittstelle kann transparent von beliebigen Anwendungen genutzt werden. Sie kommt in ihrer universellen Nutzbarkeit einem IPSec-Tunnel sehr nahe. Insbesondere ergibt sich der Vorzug, dass bei der PPP-Aushandlung dem Client wesentliche Infrastrukturmerkmale des internen Netzes mitgegeben werden können. Das gilt sowohl für den DNS-Dienst im internen Netz als auch ggf. für die korrespondierenden Windows-Namensdienste (WINS). Diese Infrastrukturmerkmale gelten für die Lebensdauer des PPP-Tunnels. Ohne PPP-Tunnel (also etwa bei einer nativen SSL-Verbindung, z. B. 4.3.4.4) sind die Einstellungen zur Namensauflösung am Remote-Client nicht dieselben wie die eines Clients im internen Netz. Ohne Hilfstechniken, z. B. hosts- oder lmhost-Dateien am Client, sind dann interne Dienste nicht mit Namen, sondern ggf. nur mit Hilfe von IP-Adressen erreichbar.

Eine Implementation dieser Forwarding-Technik ist „stunnel“.

4.3.5 Benötigte Paketfilterregeln

Die benötigten Paketfilterregeln sind nicht für alle SSL-VPN-Szenarien gleich. Hier kommt es nutzungs- und auch implementationsabhängig darauf an,

1. ob der Client mit dem zentralen Gateway ausschließlich per HTTPS verkehrt bzw. nicht unbedingt HTTPS, aber immer der TCP-Port 443 verwendet wird oder
2. ob auch noch andere Ports als Port 443 genutzt werden.

Bei ausschließlicher Nutzung des Browsers ohne Verwendung eines dedizierten SSL-Client-Plugins muss HTTPS für die am VPN beteiligten Systeme freigeschaltet werden (s. Tabelle 9: Standard-SSL-VPN-Dienste). Dasselbe gilt, wenn bei installierten Plug-In-Modulen ausschließlich der HTTPS-Port genutzt wird. Quellport und Zielport beziehen sich im Folgenden auf den Initiator der Verbindung:

Dienst	Protokoll	Quellport	Zielport
HTTPS	TCP	nicht festgelegt	443

Tabelle 9: Standard-SSL-VPN-Dienste

Hier sei beispielhaft eine Paketfilterregel für den Zugriff externer Clients auf den zentralen SSL-VPN-Service gegeben. Vorausgesetzt wird dabei, dass die Clients aus dem nicht-vertrauenswürdigen Netz mit variablen IP-Adressen auf den VPN-Server in einer DMZ zugreifen und dass der Paketfilter zwischen dem nicht-vertrauenswürdigen Netz und dem VPN-Server platziert ist und somit die Zugriffe aus dem nicht-vertrauenswürdigen Netz auf den VPN-Server filtert.

In der folgenden Tabelle sind die Variablennamen wie folgt belegt:

- $AUSSEN: IP-Adresse der Schnittstelle zum nicht-vertrauenswürdigen Netz
- $VPNSRV: IP-Adresse des VPN-Servers
- $VPNDMZ: IP-Adresse der Schnittstelle zur DMZ

HTTPS Internet – VPN-Server	iptables -A FORWARD -p TCP -i $AUSSEN -o $VPNDMZ [--dst $VPNSRV] --dport 443 --m state --state NEW,ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -p TCP -i $VPNDMZ -o $AUSSEN [--src $VPNSRV] --sport 443 --m state --state ESTABLISHED,RELATED -j ACCEPT

Bei allen anderen Implementationen kommt es darauf an, welche Ports zusätzlich genutzt werden (s. Tabelle 4, Quellport und Zielport beziehen sich auf den Initiator der Verbindung).

Dienst	Protokoll	Quellport	Zielports
HTTPS	TCP	nicht festgelegt	443
Andere Dienste	TCP	nicht festgelegt	implementations- und konfigurationsabhängig

Tabelle 10: SSL-VPN bei erweiterter Nutzung

Wird hingegen ausschließlich eine vollständige Integration eines Clients oder zweier Netze genutzt, beispielsweise beim Tunneln einer PPP-Verbindung durch SSL, hängt es von der Implementation ab, welcher Port verwendet wird (s. Tabelle 11, Quellport und Zielport beziehen sich auf den Initiator der Verbindung).

Dienst	Protokoll	Quellport	Zielports
Andere Dienste	TCP	nicht festgelegt	implementations- und konfigurationsabhängig

Tabelle 11: Spezifisches SSL-VPN

4.3.6 Checkliste sichere Konfiguration

Im Folgenden finden sich Checklisten zur sicheren SSL-VPN-Konfiguration.

Anforderung	erfüllt	
	ja	nein
Der Schlüsselaustausch ist mit einem sicheren Verfahren mit ausreichender Schlüssellänge durchgeführt worden.		
Sichere Verschlüsselungsverfahren mit ausreichender Schlüssellänge werden verwendet.		
Es werden ausschließlich sichere Authentisierungsverfahren verwendet.		
Bei Verwendung von Zertifikaten zur Authentisierung wird während des Authentisierungsvorgangs der Status des Zertifikats bei einer PKI überprüft.		
Timeouts sind nicht zu groß gewählt worden.		

Tabelle 12: Sichere SSL-VPN-Konfiguration (allgemein)

Da SSL-VPN-Clients nicht immer der Kontrolle der eigenen Organisation unterliegen (z. B. Zugriff auf den Client durch Dritte), sollten speziell für VPN-Clients folgende Punkte betrachtet werden:

Anforderung	erfüllt	
	ja	nein
Authentisierungsschlüssel werden nicht in einer unverschlüsselten Form auf dem System gespeichert.		
Für den Schutz der Authentisierungsschlüssel wurde ein sicheres Passwort gewählt.		
Direkte Verbindungen außerhalb des Tunnels zu nicht-vertrauenswürdigen Systemen („Split-Tunneling“) werden während einer VPN-Sitzung unterbunden.		
Clientsysteme genügen dem sonst im Organisationsnetz üblichen Schutzniveau bezüglich Sicherheit vor Viren und Trojanischen Pferden.		
Clientsysteme werden bei direkter Verbindung mit nicht-vertrauenswürdigen Netzen durch einen Paketfilter gesichert.		

Tabelle 13 Sichere SSL-VPN-Konfiguration der Clients

An die VPN-Gateways werden folgende Anforderungen gestellt:

Anforderung	erfüllt	
	ja	nein
Es dürfen ausschließlich erforderliche Dienste auf der äußeren Netzschnittstelle aus dem nicht-vertrauenswürdigen Netz erreichbar sein.		
Verbindungen werden lediglich zu den notwendigen Systemen und Diensten erlaubt. Diese Anforderung ist möglicherweise nicht in allen Einsatzszenarien praktikabel.		
Die im internen Netz sichtbaren IP-Adressen der sich verbindenden VPN-Clients stammen aus einem definierten Adressbereich (nur relevant bei vollständiger Client-Integration, z. B. über eine PPP-Verbindung im SSL-Tunnel).		

Tabelle 14 Sichere SSL-VPN-Konfiguration der VPN-Gateways

4.3.7 Häufig auftretende Probleme

SSL-VPNs sind im Vergleich zu IPSec-VPNs relativ unproblematisch.

Da SSL weder IP-Informationen noch auf Transportebene schützt, sondern lediglich die Anwendungsdaten, gibt es keine NAT-Probleme. Auch gibt es bei SSL nicht die Fülle der IPSec-inhärenten und bei einer erwünschten Verbindung konsistent auf beiden beteiligten Seiten abzustimmenden Konfigurationsparameter.

Einen weiteren nicht zu unterschätzenden Faktor beim Einsatz von SSL-VPN stellt die Tatsache dar, dass SSL-VPN im Regelfall nur zur Anbindung von Clients an eine ausgesuchte Teilmenge intern verfügbarer Dienste mit Browser-Technologien genutzt wird und nicht für transparente Netzkopplungen. Probleme mit der Interoperabilität, die beispielsweise bei der Verwendung von SSL-Plugins unterschiedlicher Hersteller auftreten könnten, sind unter diesem Aspekt relativ selten.

Folgende Probleme im Zusammenhang mit SSL könnten auftreten:

- Die SSL-Implementationen haben sich in der Vergangenheit als stärker fehlerbehaftet gezeigt als andere VPN-Implementationen (z. B. IPSec).
- Die Sicherheit von SSL-VPNs wird zum Teil auf den Anwender verlagert, da dieser unerwünschte Verbindungen anhand der Zertifikate erkennen und ablehnen muss.
- Existierende, öffentliche Zertifikatsstrukturen sollten bei hohem Schutzbedarf kritisch betrachtet werden. Es sollte nur solchen Zertifizierungsstellen vertraut werden, die eine umfassende Prüfung eines Zertifikatsantrags vornehmen und nicht beispielsweise nur auf der Basis gegenseitigen Vertrauens bzw. gegenseitiger Bestätigung der Vetrauenswürdigkeit Zertifikate ausstellen.
- Zum Betrieb von SSL-VPN mit vielen Nutzern ist in der Regel eine eigene Zertifikatsstruktur erforderlich.
- Zum sicheren Betrieb von SSL-VPNs müssen sowohl Client- als auch Server-Zertifikate verwendet werden. Vorkonfiguriert ist beim Einsatz von Standardprodukten meist nur die Verwendung von Server-Zertifikaten.
- Zur Verwendung von Client-Zertifikaten müssen die Zertifikate auf die Clients verteilt werden, was erheblichen Administrationsaufwand mit sich bringen kann.
- SSL wurde nur zum Betrieb mit TCP entwickelt. Probleme können bei der Verwendung von UDP entstehen.

4.4 Point-To-Point-Tunneling-Protocol (PPTP)

PPTP ist eine bereits in älteren Microsoft-Betriebsystemen enthaltene Möglichkeit, ohne Einsatz von Zusatzsoftware VPNs aufzubauen. Die Microsoft-Implementierung von PPTP hat sich als sicherheitstechnisch mangelhaft erwiesen, unter anderem wegen gravierender kryptographischer Schwachstellen insbesondere in Zusammenhang mit schwachen Passwörtern (z. B. http://www.schneier.com/paper-pptpv2.html).

Da zudem die Authentifizierung bei PPTP auf Passwörtern basiert und eine zertifikatsgeschützte Authentifizierung nicht ohne weiteres ermöglicht, wird der Einsatz von PPTP als VPN-Lösung nicht empfohlen.

4.5 Vergleich der VPN-Varianten

In diesem Abschnitt werden die zuvor vorgestellten VPN-Varianten in tabellarischer Form bezüglich ihrer Eigenschaften verglichen. Hierbei muss beachtet werden, dass hier Standards wie IPSec und PPP/L2TP/IPSec mit einer Reihe von unstandardisierten SSL/TLS-Lösungen verschiedener Hersteller (SSL-VPN) verglichen werden.

In Tabelle 15 werden folgende Bezeichnungen verwendet:

x vorhanden

\- nicht vorhanden

h herstellerspezifisch

VPN-Typ / **Merkmal**		**IPSec**	**PPP/L2TP/ IPSec**	**SSL-VPN**			
				„Clientless“	**Client[1)]**	**Anwendung nutzt SSL-Forwarder**	**PPP über SSL**
Transport-Protokoll		(AH), ESP, UDP[2)]	ESP, UDP[2)]	HTTPS	SSL/TCP	SSL/TCP	SSL/TCP
Tunnel/Transport von	nicht-IP	-	x	-	-	h	x
	TCP	x	x	-	x	x	x
	UDP	x	x	-	h	x	x
	ICMP	x	x	-	-	x	x
	andere IP-Unicasts	x	x	-	-	x	x
	IP-Broadcasts	-	x	-	-	h	x
NAT-verträglich		h	h[3)]	x	x	x	x
HTTP-Proxy-Traversal		-	-	x	h	h	-
Komprimierung		h	h[3)]			h	h
LAN-LAN-Kopplung möglich		x	x	-	-	h	x
Clientintegration: Software notwendig		x	x	-	x	x	x
Externe Authentisierung möglich		h[4)]	h/-/h[4)]	h	h	h	h
Interoperabilität mit Drittherstellern		h	h	x	-	-	h

Tabelle 15: Vergleich der VPN-Varianten

1) Hier werden sowohl fest zu installierende, dedizierte SSL-Clients als auch dynamisch geladene ActiveX- oder Java-SSL-Clients zusammengefasst.

2) In der Regel nur mit NAT-Traversal möglich, da hier üblicherweise IPSec im Transport-Mode verwendet wird.

3) Abhängig von der IPSec-Implementierung.

4) Mithilfe von nicht-standardisierten Verfahren wie XAuth und HybridAuth.

5. Grundlageninformationen zur Integration eines VPN in ein Sicherheitsgateway

In den folgenden Unterkapiteln werden die Schutzmöglichkeiten von Sicherheitsgateways, Kriterien zur Feststellung des Schutzbedarfs und Gruppierungsmöglichkeiten verschiedener VPN-Szenarien aufgelistet. Diese Informationen sind beim Entwurf von VPN-Lösungen von besonderer Relevanz und sollen auf die Empfehlungen zur Integration von VPN in den Kapiteln 6 und 7 vorbereiten.

5.1 Schutzmöglichkeiten von Sicherheitsgateways

Bei der Integration von VPN-Komponenten in bestehende Sicherheitsgateways ist zu berücksichtigen, welche Schutzfunktionen zur Absicherung der VPN-Komponenten genutzt werden können und wie die Komponenten zur Erzielung welchen Schutzes eingebaut werden können.

Zur Absicherung vertrauenswürdiger Netze mit hohem Schutzbedarf gegen nicht-vertrauenswürdige Netze wird vom BSI ein dreistufiges Sicherheitssystem empfohlen (s. http://www.bsi.de/fachthem/sinet/loesungen_netze/konzsichgw.htm). Ein solches setzt sich aus den folgenden Komponenten zusammen, wobei diese hier jeweils mit Schutzmöglichkeiten mit VPN-Bezug betrachtet werden:

- Äußerer Paketfilter
  Der äußere Paketfilter beschränkt die aus nicht-vertrauenswürdigen Netzen eingehenden Verbindungsinitiierungen auf die erlaubten Dienste.
  Bei Verbindungen aus nicht-vertrauenswürdigen Netzen kann der äußere Paketfilter höchstens die Ziel-IP-Adresse (z. B. des VPN-Gateways) und den genutzten Port (z. B. Port 443 bei SSL) kontrollieren. Der Paketfilter kontrolliert häufig nicht, ob über diesen Port tatsächlich mit dem erwarteten Protokoll kommuniziert wird oder ob gar unerlaubte Protokolle getunnelt werden. Der Paketfilter kann jedoch wirksam Portscans und Angriffe auf problematische Standard-Betriebssystem-Ports abwehren. Zusätzlich kann ein Paketfilter prüfen, ob ein Paket an der Schnittstelle des Paketfilters ankommt, an die es laut Absender-IP-Adresse hingehört (Anti-Spoofing), d. h., es wird kontrolliert, ob Pakete aus dem nicht-vertrauenswürdigen Netz auf der äußeren Schnittstelle und Pakete aus dem vertrauenswürdigen Netz auf der inneren Schnittstelle eintreffen.
- Application-Level-Gateway (ALG)
  Das Application-Level-Gateway kontrolliert die Nutzung der Protokolle auf Anwendungsebene und trennt die direkte Kommunikation zwischen zwei Netzen durch die Proxy-Funktionalität. Pakete werden nicht über das Gateway geroutet, zur Weiterleitung der Pakete stellt der ALG eine neue Verbindung mit dem gewünschten Zielsystem her. Ein- und ausgehende Pakete werden über getrennte TCP/IP-Stacks angenommen und weitergereicht. Die Header werden ausgetauscht, um Angriffe auf Basis spezieller Headerdaten auszuschließen.
  Werden VPN-Verbindungen über ein Sicherheitsgateway geleitet, kann ein ALG auf Port- und Protokollebene zunächst keinen größeren Schutz bieten als ein Paketfilter, da der verschlüsselte Datenstrom nicht geprüft werden kann. Produktabhängig können jedoch SSL-Proxies eingesetzt werden, oder der VPN-Tunnel kann auf dem ALG terminiert werden, so dass die im Tunnel genutzten Dienste im Klartext vorliegen und auf Anwendungsebene geprüft werden können.
- Innerer Paketfilter
  Der innere Paketfilter schützt das interne Netz für den Fall, dass das Application-Level-Gateway oder Systeme in geschützten Zonen der Sicherheitsgateway-Architektur kompromittiert werden. Der Paketfilter verhindert, dass die unverschlüsselte, interne Kommunikation bei der Übernahme eines ALG abgehört und die Informationen für weitere Angriffe weiterverwendet werden können. Broadcasts erreichen das ALG je nach Konfiguration des Paketfilters nicht. Der innere Paketfilter schützt das ALG zudem vor Innentätern.
  Da über den inneren Paketfilter häufig unverschlüsselte Verbindungen geleitet werden (die

Verschlüsselung erfolgt oft erst an anderer Stelle), kann er kontrollieren, welche Dienste aus dem internen Netz genutzt werden. Diese Kontrolle ist nur auf Adress- und Portebene möglich.

Je nach eingesetzter Krypto-VPN-Variante müssen zum VPN-Gateway unterschiedliche Ports zugelassen werden, damit der VPN-Kanal aufgebaut und Daten übertragen werden können. Die benötigten Regeln werden in Abschnitt 4.1.7 (IPSec-Tunnel) und 4.3.5 (SSL-Tunnel) beschrieben.

Verschiedene Platzierungsvarianten von Paketfiltern und ALGs werden in Kapitel 6 diskutiert.

5.2 Sicherheitsgrundfunktionen von VPN-Produkten

Bei der Realisierung von Sicherheitsgateways und deren Revision muss sichergestellt werden, ob geforderte Sicherheitsfunktionen auch tatsächlich vom ausgewählten Produkt erfüllt werden können. Die Anforderungen an VPN-Produkte können dabei beispielsweise anhand von fünf Funktionsklassen beurteilt werden. Die hier vorgestellten Klassen behandeln nur die Besonderheiten von VPN-Produkten gegenüber anderen Sicherheitsprodukten:

- Identifikation und Authentisierung
  Hierunter fallen die Identifikation und Authentisierung von Systemen untereinander, Systemen gegenüber Benutzern und Benutzern gegenüber Systemen und Anwendungen.
- Datenflusskontrolle
  Im Zusammenhang mit Netzübergängen ist der Begriff Datenflusskontrolle als Kontrolle der Kommunikation zu verstehen, die über ein Sicherheitsgateway erfolgen darf.

Die Wirksamkeit der Datenflusskontrolle kann u. a. nach der Leistungsfähigkeit der Kontrollalgorithmen geordnet werden. Dabei gilt:

- Eine Kontrolle auf Anwendungsebene durch ein Application-Level-Gateway ist höher zu bewerten als eine Paketfilterung auf niedrigeren Protokollebenen, da auf Anwendungsebene zusätzlich die übertragenen Daten kontrolliert werden können.
- Eine benutzerbezogene Kontrolle der Dienstnutzung ist höher zu bewerten als eine maschinenbezogene Kontrolle, da bei einer Kontrolle der Dienstnutzung auf Benutzerebene das Prinzip der niedrigsten Privilegierung („least privilege principle“) besser durchsetzbar ist. Dies ist wesentlich bei Mehrbenutzersystemen und Benutzern mit unterschiedlichem Kommunikationsbedarf auf einer Maschine.
- Beweissicherung
  Mit Hilfe der Beweissicherung können netzspezifische Ereignisse aufgezeichnet und ausgewertet werden. Die aufgezeichneten Ereignisse dienen u. a.:

- der frühzeitigen Erkennung sicherheitsrelevanter Vorkommnisse
- als Beweisgrundlage für eine spätere Tatverfolgung
- der Fehlerbehebung beim Auftreten von technischen Problemen

Die Stärke der Beweissicherung kann nach dem Umfang der aufgezeichneten Daten geordnet werden. Bei der Umsetzung der Beweissicherung müssen datenschutzrechtliche Aspekte betrachtet werden.

- Übertragungssicherung
  Bei der Übertragungssicherung kommen Mechanismen zum Einsatz, welche die Vertraulichkeit und Integrität der Daten sichern. Dies kann durch den Einsatz maschinen- oder personenbezogener Verschlüsselung erreicht werden. Im Zusammenhang mit dieser Studie wird unter der maschinenbezogenen Verschlüsselung die Sicherung der Datenübertragung zwischen zwei Sicherheitsgateways verstanden.
  Die maschinenbezogene Verschlüsselung wird in den unteren Protokollschichten der Netzsoftware eingesetzt. Sie ist damit in der Lage, sämtliche von und zu dem jeweiligen

Netzknoten (Endsystem oder Netzkomponente) übertragenen Daten zu sichern. Dies schließt auch Netzdienste und Protokollinformationen höherer Protokollschichten ein.

- Schlüsselmanagement
  Das Schlüsselmanagement stellt Mechanismen für die Übertragungssicherung bereit, um geheime und öffentliche Schlüssel für die kryptographischen Funktionen zu verteilen.
  Anhand dieser Sicherheitsgrundfunktionen werden in Kapitel 8 grundlegende Empfehlungen für eine sichere Implementation eines VPN-Gateways aufgelistet.

5.3 Gruppierung von Szenarien

Nach dem Aufbau eines VPN-Kanals können von den Client-Systemen, abhängig vom gewähltem VPN-Typ, alle Dienste genutzt werden, die an den Tunnelendpunkten angeboten werden. Je nach Einsatzszenario kann die explizite Sperrung einzelner Dienste erforderlich sein, wobei beim Entwurf gruppiert werden kann nach Szenarien, bei denen die Clients unter eigener Kontrolle stehen, und Szenarien, bei denen die Client-Systeme unter fremder Kontrolle stehen bzw. Dienste auf Administratorebene genutzt werden.

5.3.1 Clients unter eigener Kontrolle

Unter diese Gruppe fallen die folgenden Szenarien:

- mobiler Mitarbeiter
- Heimarbeitsplatz
- Standortvernetzung
- WLAN-Absicherung

Bei den Szenarien dieser Gruppe ist es häufig erforderlich, die komplette Bandbreite an Diensten zu erlauben, d. h. eine transparente Anbindung bereitzustellen. Der Anwender soll so behandelt werden, als ob er sich direkt im internen Netz befindet. Durch die Art und Vielfalt der genutzten Dienste und die Vertrauenswürdigkeit der Anwender ist eine Prüfung der Dienste auf Anwendungsebene nicht unbedingt notwendig.

Eine weitere Gruppe wird durch die Szenarien gebildet, bei denen die Client-Systeme unter fremder Kontrolle stehen bzw. Dienste auf Administratorebene genutzt werden.

5.3.2 Client-Systeme unter fremder Kontrolle oder Dienstnutzung auf Administratorebene

Unter diese Gruppe fallen die folgenden Szenarien:

- Anbindung von Kunden und Partnern
- Fernwartung

Bei den Einsatzszenarien dieser Gruppe handelt es sich entweder um fremde Mitarbeiter oder um Dienste, die Zugriffe auf Betriebssystemebene erlauben. Die benötigten Dienste lassen sich genau eingrenzen und sind auf Anwendungsebene zu prüfen. Dies ist problematisch bei der Nutzung der Fernwartungs-Dienste SSH bzw. HTTPS, da der Datenstrom dieser verschlüsselten Verbindungen nicht kontrolliert werden kann, falls er bis zum Endsystem verschlüsselt ist. Eine Filterung der tatsächlich innerhalb von SSH und HTTPS genutzten Dienste ist am Sicherheitsgateway bei Verwendung von Ende-zu-Ende-Sicherheit nicht möglich. Aufgrund der Abhörgefahr bei den Klartext-Alternativen (telnet und HTTP) wird trotzdem empfohlen, zu Fernwartungszwecken SSH bzw. HTTPS einzusetzen. Zur Minimierung der Risiken ist das Zielsystem entsprechend sicher zu platzieren und zu konfigurieren.

Beim Einsatz von HTTPS ist eine zwischenzeitliche Entschlüsselung am Sicherheitsgateway möglich, so dass der Datenstrom gefiltert werden kann. Hierbei ist zu beachten, dass das Zielsystem dann nur noch Verbindungen mit der Absenderadresse und dem Zertifikat des Sicherheitsgateways erhält, was zu Problemen bei der Authentisierung unterschiedlicher Verbindungen am Zielsystem führen kann.

Auch bei Verwendung von SSH ist es denkbar, die Verbindung nicht auf dem Zielsystem terminieren zu lassen, sondern auf einem vorgeschalteten Rechner. Dieser könnte dann mittels eines Zwangs-Proxies bestimmte Befehle unterdrücken, die ein entfernter Nutzer auf dem Zielsystem ausführen möchte. Die Proxy-Funktionalität muss dabei in der Regel selbt programmiert werden.

6. Integration von VPN-Komponenten in Sicherheitsgateways

Dieser Abschnitt beschreibt die Vor- und Nachteile der verschiedenen Integrationsmöglichkeiten des VPN-Gateways innerhalb des dreistufigen Sicherheitssystems.

Die Platzierung ist abhängig von mehreren Faktoren:

- Schutzbedarf des VPN-Gateways vor Angriffen aus dem nicht-vertrauenswürdigen Netz
- Notwendigkeit der Kontrolle und Flusssteuerung der Zugriffe aus dem nicht-vertrauenswürdigen Netz auf Systeme und Dienste im vertrauenswürdigen Netz
- Schutzbedarf der übertragenen Daten

Die Vor- und Nachteile der einzelnen Architekturen werden diskutiert und die resultierenden Empfehlungen kompakt in einer Matrix dargestellt (siehe Abschnitt 6.15 auf Seite 77).

Die nachfolgende Abbildung zeigt die unterschiedlichen Integrationsmöglichkeiten von VPN-Gateways mit einer Netzschnittstelle. Die Nummerierung der einzelnen Integrationsvarianten entspricht jeweils dem zu der Platzierungsvariante gehörenden Kapitel in diesem Dokument.

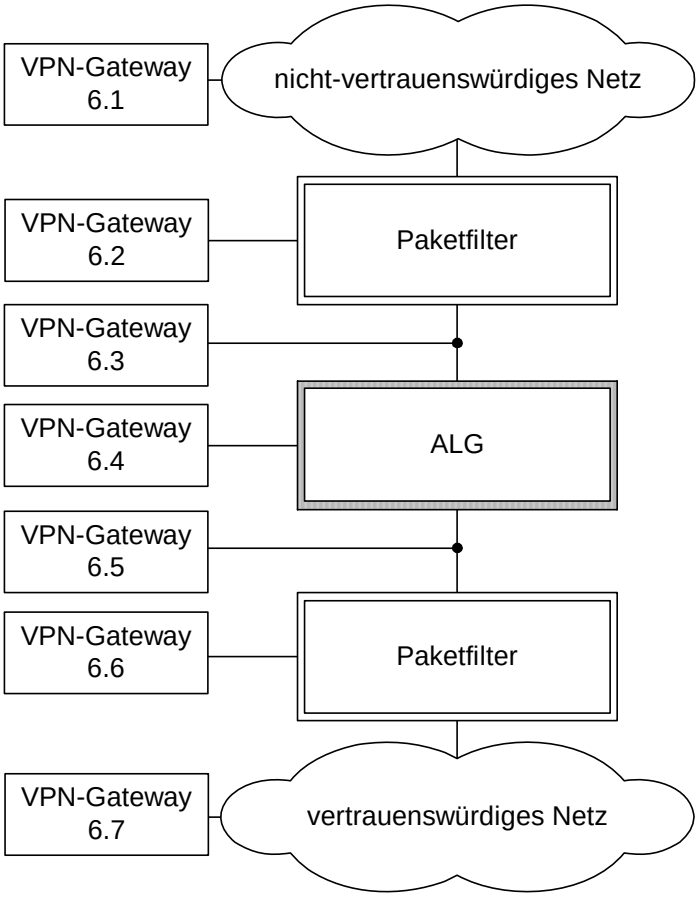


Abbildung 30 Platzierungsvarianten des VPN-Gateways mit einer Schnittstelle

Produktabhängig können VPN-Gateways mit zwei Netzschnittstellen eingesetzt werden. Die zusätzlich zum Paketfilter mit einer Netzschnittstelle möglichen Platzierungsvarianten werden nachfolgend dargestellt:

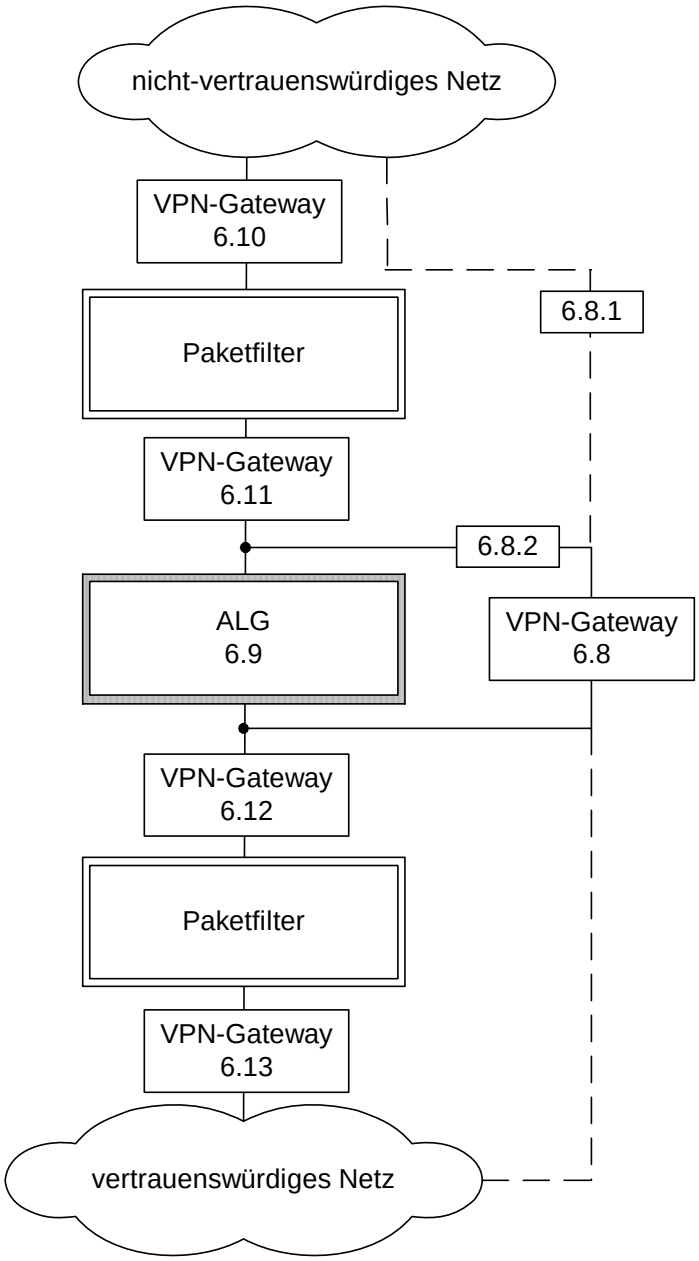


Abbildung 31 Platzierungsvarianten des VPN-Gateways mit zwei Schnittstellen

Die Varianten und weiteren Kombinationen sind für alle Krypto-Varianten gültig und werden nachfolgend detailliert diskutiert. Die Empfehlungen sind möglicherweise nicht in jedem Anwendungszusammenhang (sicherheits-)technisch sinnvoll und somit dem jeweiligen Einsatzzweck anzupassen.

Bei der Bewertung der Platzierungsvarianten werden die unter Abschnitt 5.1 formulierten, allgemeinen Schutzmöglichkeiten eines Sicherheitsgateways berücksichtigt.

6.1 VPN-Komponente vor dem externen Paketfilter

Voraussetzung: keine

Vorteile:

- Diese Platzierungsvariante ist lediglich für den Betrieb der VPN-Komponente durch einen Dienstleister denkbar.

Nachteile:

- Die VPN-Komponente steht ungeschützt im nicht-vertrauenswürdigen Netz und ist dadurch insbesondere auf Betriebssystemebene angreifbar. Dem kann nur durch Einsatz aktueller Softwareversionen, Härtung der Konfiguration und Deaktivierung aller nicht benötigten Dienste begegnet werden.
- Falls das VPN zur Absicherung des Zugriffs auf Systeme im vertrauenswürdigen Netz dient, muss der entschlüsselte Datenverkehr auf dem Weg in das vertrauenswürdige Netz den äußeren Paketfilter, das ALG und den inneren Paketfilter passieren. Somit sind umfangreiche Freischaltungen auf allen Komponenten notwendig, da der entschlüsselte Verkehr möglicherweise viele Verbindungen umfasst. U. U. muss an dieser Stelle auch die Freischaltung bzw. Sperrung der Kommunikation für einzelne Rechner oder Server des vertrauenswürdigen Netzes erfolgen.
- Die unverschlüsselten Daten werden vom VPN-Gateway über das nicht-vertrauenswürdige Netz übertragen, können also hier gegebenenfalls mitgelesen werden, falls keine dedizierte Leitung zwischen VPN-Gateway und dem Sicherheitsgateway genutzt wird.
- Die Administration wird erschwert, weil das VPN-Gateway zwar unter eigener Kontrolle steht, jedoch extern untergebracht ist. Ein getrenntes Management-Netz ist nicht möglich, so dass Management-Verbindungen zum VPN-Gateway in das nicht-vertrauenswürdige Netz erforderlich sind.
- Der externe Paketfilter ist nicht in der Lage zu erkennen, ob unverschlüsselte Verbindungen tatsächlich vom VPN-Gateway stammen oder von einem Angreifer, der die offizielle IP-Adresse des VPN-Gateways als Absenderadresse nutzt (IP-Spoofing). Die Angreifer erhalten zwar keine Rückpakete, jedoch sind aufgrund der fehlenden Filtermöglichkeiten Spoofing- und Denial-of-Service-Angriffe möglich.

Empfehlung:

Die Aufstellung des VPN-Gateways vor dem externen Paketfilter wird aufgrund der Vielzahl der Nachteile nicht empfohlen.

6.2 VPN-Komponente am externen Paketfilter

Voraussetzung: Das VPN-Gateway muss mit einer Netzschnittstelle betrieben werden können.

Vorteile:

- Durch die Anbindung des VPN-Gateways an den äußeren Paketfilter wird das VPN-System gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Der äußere Paketfilter schützt im Vergleich zu Variante 6.1 zusätzlich gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Das VPN-Gateway wird aus dem nicht-vertrauenswürdigen Netz direkt angesprochen und ist somit auch direkt angreifbar, wenn Konfigurationsfehler im äußeren Paketfilter vorliegen.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.
- Falls das VPN zur Absicherung des Zugriffs auf Systeme im vertrauenswürdigen Netz dient, muss der entschlüsselte Datenverkehr, der aus mehreren Kommunikationsbeziehungen bestehen kann, auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Es sind ggf. umfangreiche Freischaltungen notwendig.

Empfehlung: Aufgrund der erforderlichen Öffnung des Application-Level-Gateways wird die Aufstellung des VPN-Gateways am externen Paketfilter nicht empfohlen.

6.3 VPN-Komponente hinter dem externen Paketfilter

Voraussetzung: Das VPN-Gateway muss mit einer Netzschnittstelle betrieben werden können.

Vorteile:

- Bei der Platzierung des VPN-Gateways zwischen dem äußeren Paketfilter und dem Application-Level-Gateway wird das VPN-System gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Der äußere Paketfilter schützt zusätzlich im Vergleich zu Variante 6.1 gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Das VPN-Gateway wird aus dem nicht-vertrauenswürdigen Netz direkt angesprochen und ist somit auch direkt angreifbar, wenn Konfigurationsfehler im äußeren Paketfilter vorliegen.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.
- Falls das VPN zur Absicherung des Zugriffs auf Systeme im vertrauenswürdigen Netz dient, muss der entschlüsselte Datenverkehr auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Es sind ggf. umfangreiche Freischaltungen notwendig.

Empfehlung: Aufgrund der erforderlichen Öffnung des Application-Level-Gateways wird die Aufstellung des VPN-Gateways zwischen dem externen Paketfilter und dem Application-Level-Gateway nicht empfohlen.

6.4 VPN-Komponente am Application-Level-Gateway

Voraussetzung: Das VPN-Gateway muss mit einer Netzschnittstelle betrieben werden können.

Vorteile:

- Je nach Implementierung des ALG können VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz nur auf das ALG zugelassen werden. Das ALG leitet die Verbindungen dann zum VPN-Gateway weiter. Das VPN-Gateway, das mit dieser Methode keine offizielle IP-Adresse mehr braucht, ist somit nur für den VPN-Dienst erreichbar. Konfigurationsfehler des VPN-Gateways werden evtl. durch das ALG abgefangen, da dieses gegenüber dem nicht-vertrauenswürdigen Netz als Stellvertreter des VPN-Gateways auftritt.
- Der äußere Paketfilter schützt zusätzlich im Vergleich zu Variante 6.1 gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden.
- Der entschlüsselte Datenverkehr muss auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Da entschlüsselte Verbindungen nur an der DMZ-Schnittstelle des ALG und nicht an der Schnittstelle des ALG zum nicht-vertrauenswürdigen Netz erlaubt werden, ist ein unberechtigter Verbindungsaufbau aus dem nicht-vertrauenswürdigen Netz gegenüber den vorangehenden Varianten deutlich erschwert. Dieser Schutz verringert sich dann, wenn Standard-Klartext-Verkehr (z. B. HTTP, SMTP) aus dem nicht-vertrauenswürdigen Netz in das vertrauenswürdige Netz gestattet ist, weil in diesem Fall eine Verbindung ohne „Umweg“ über eine DMZ wieder ermöglicht wird.
- Der entschlüsselte, in das vertrauenswürdige Netz gerichtete Datenverkehr erreicht das ALG über die Schnittstelle zur DMZ und ist nicht mehr mit dem Standard-Verkehr (z. B. HTTP, SMTP) aus dem nicht-vertrauenswürdigen Netz vermischt. Die Konfiguration des ALG ist dadurch wesentlich übersichtlicher, weil diese in der Regel für jede Schnittstelle getrennt vorgenommen wird.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Die Weiterleitung von VPN-Verbindungen durch das ALG kann produktspezifisch problematisch sein, z. B. ist es bei manchen ALGs nicht möglich, reines IPSec (ESP, AH) durchzulassen. In diesen Fällen ist zu prüfen, ob Ersatzlösungen (z. B. IPSec über UDP/500) möglich sind.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.

Empfehlung: Aufgrund der realisierbaren Schutzmechanismen wird die Aufstellung des VPN-Gateways in einem separaten Teilnetz am Application-Level-Gateway empfohlen.

6.5 VPN-Komponente hinter dem Application-Level-Gateway

Voraussetzung: Das VPN-Gateway muss mit einer Netzschnittstelle betrieben werden können.

Vorteile:

- Bei der Platzierung des VPN-Gateways zwischen dem Application-Level-Gateway und dem internen Paketfilter wird das System durch den externen Paketfilter und das ALG gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Je nach Implementierung des ALG können VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz nur auf das ALG zugelassen werden. Das ALG leitet die Verbindungen dann zum VPN-Gateway weiter. Das VPN-Gateway, das mit dieser Methode keine offizielle IP-Adresse mehr braucht, ist somit nur für den VPN-Dienst erreichbar. Konfigurationsfehler des VPN-Gateways werden evtl. durch das ALG abgefangen, da dieses gegenüber dem nicht-vertrauenswürdigen Netz als Stellvertreter des VPN-Gateways auftritt.

- Bei einer LAN-LAN-VPN-Kopplung ist nur die Freischaltung eines Proxies für die VPN-Verbindung erforderlich. Die Freischaltung vieler Proxies für den unverschlüsselten Datenverkehr ist nicht erforderlich.
- Der äußere Paketfilter schützt zusätzlich im Vergleich zu Variante 6.1 gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Das ALG muss eingehende und ausgehende VPN-Verbindungen weiterleiten, ohne die Inhalte der Verbindungen prüfen zu können.
- Der entschlüsselte Datenverkehr muss auf dem Weg in das vertrauenswürdige Netz nur noch den inneren Paketfilter passieren. Es ist keine Kontrolle der unverschlüsselten Verbindungen auf Anwendungsebene mehr möglich.
- Die Weiterleitung von VPN-Verbindungen durch das ALG kann produktspezifisch problematisch sein, z. B. ist es bei manchen ALGs nicht möglich, reines IPSec (ESP, AH) durchzulassen. In diesen Fällen ist zu prüfen, ob Ersatzlösungen (z. B. IPSec über UDP/500) möglich sind.

Empfehlung: Aufgrund der erforderlichen Freischaltung des Application-Level-Gateways für von außen eingehende VPN-Verbindungen wird die Platzierung der VPN-Komponente zwischen dem Application-Level-Gateway und dem internen Paketfilter nicht empfohlen.

6.6 VPN-Komponente am internen Paketfilter

Diese Variante entspricht sicherheitstechnisch weitestgehend der im Kapitel 6.5 vorgestellten Lösung, so dass die gleichen Vor- und Nachteile sowie Empfehlungen gelten.

6.7 VPN-Komponente im LAN

Voraussetzung: Das VPN-Gateway muss mit einer Netzschnittstelle betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways im internen Netz wird das System durch beide Paketfilter und das ALG gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Je nach Implementierung des ALG können VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz nur auf das ALG zugelassen werden. Das ALG leitet die Verbindungen dann zum VPN-Gateway weiter. Das VPN-Gateway, das mit dieser Methode keine offizielle IP-Adresse mehr braucht, ist somit nur für den VPN-Dienst erreichbar.
- Konfigurationsfehler des VPN-Gateways werden evtl. durch das ALG abgefangen, da dieses gegenüber dem nicht-vertrauenswürdigen Netz als Stellvertreter des VPN-Gateways auftritt.
- Der äußere Paketfilter schützt zusätzlich im Vergleich zu Variante 6.1 gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Das ALG und die Paketfilter müssen eingehende und ausgehende VPN-Verbindungen weiterleiten, ohne die Inhalte der Verbindungen prüfen zu können.Der entschlüsselte Datenverkehr kann nicht mehr kontrolliert und eingeschränkt werden, so dass die VPN-Clients einen kompletten Zugriff auf das interne Netz erhalten.
- Die Weiterleitung von VPN-Verbindungen durch den ALG kann produktspezifisch problematisch sein, z. B. ist es bei manchen ALGs nicht möglich, reines IPSec (ESP, AH) durchzulassen. In diesen Fällen ist zu prüfen, ob Ersatzlösungen (z. B. IPSec über UDP/500) möglich sind.

Empfehlung: Aufgrund der erforderlichen Freischaltung des Application-Level-Gateways für von außen eingehende VPN-Verbindungen wird die Platzierung der VPN-Komponente zwischen dem Application-Level-Gateway und dem internen Paketfilter nicht empfohlen.

6.8 VPN-Komponente parallel zum Sicherheitsgateway

Bei der Integration der VPN-Komponenten parallel zum Sicherheitsgateway sind zwei Varianten zu berücksichtigen:

Ein dedizierter VPN-Zugang, der unabhängig von dem eigentlichen Zugang in das nicht-vertrauenswürdige Netz ist (gestrichelte Linie in Abbildung 31).

Ein Gateway-System, das parallel zum Application-Level-Gateway zwischen dem äußeren und inneren Paketfilter platziert wird. In diesem Fall wird die VPN-Gateway-Funktionalität parallel zum Application-Level-Gateway betrieben. Das System ist durch den äußeren Paketfilter geschützt, Verbindungen, die aus dem Tunnel ins interne Netz initiiert werden, können durch den internen Paketfilter kontrolliert werden.

6.8.1 Dedizierter VPN-Zugang

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Der VPN-Zugang ist komplett vom Sicherheitsgateway-System getrennt, so dass die Komponenten des Sicherheitsgateway-Systems nicht mit den VPN-Verbindungen belastet werden.
- Es entfällt die Freischaltung der Paketfilter und des ALG nicht nur für das VPN-Protokoll, sondern auch für evtl. notwendige Protokolle zum Schlüsselaustausch.
- Die Konfiguration des ALG und der Paketfilter ist durch die Trennung vom VPN-Verkehr übersichtlicher als bei den anderen vorgestellten Varianten.
- Die Konfiguration des VPN-Gateways ist möglich, ohne Rücksicht auf die Konfiguration der Paketfilter bzw. des ALG nehmen zu müssen. Es existieren also keine einschränkenden Konfigurationen oder technischen Rahmenbedingungen, die sich auf die Konfiguration des VPN-Gateways auswirken könnten.
- Der Einsatz des VPN-Gateways ist unabhängig von den verwendeten Produkten für ALGs und Paketfilter.
- Bei Ausfall eines Paketfilters oder des ALG kann das VPN u. U. weiter betrieben werden.

Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Beim dedizierten VPN-Zugang steht die VPN-Komponente ungeschützt im Internet. Das System ist dadurch insbesondere auf Betriebssystemebene angreifbar. Dem ist an dieser Stelle nur durch aktuelle Softwareversionen, eine gehärtete Konfiguration und das Deaktivieren aller nicht benötigten Dienste zu begegnen.
- Durch die Platzierung des VPN-Gateways im nicht-vertrauenswürdigen Netz und durch die Parallelschaltung des VPN-Gateways zum ALG besteht prinzipiell eine Möglichkeit zur Umgehung der Paketfilter und des ALG.
- Der entschlüsselte Datenverkehr kann nicht mehr kontrolliert und eingeschränkt werden, so dass die VPN-Endpunkte im nicht-vertrauenswürdigen Netz einen kompletten Zugriff auf das interne Netz erhalten.

Empfehlung: Aufgrund der fehlenden Schutzmöglichkeiten des VPN-Gateways und fehlender Möglichkeiten zur Kontrolle der unverschlüsselten Verbindungen wird die Anbindung der VPN-Komponente an einen dedizierten VPN-Zugang nicht empfohlen.

6.8.2 VPN-Komponente zwischen externem und internem Paketfilter

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Bei der Anbindung der äußeren Schnittstelle des VPN-Gateways zwischen dem äußeren Paketfilter und dem Application-Level-Gateway wird das VPN-System gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Der VPN-Zugang ist vom Application-Level-Gateway getrennt, so dass diese Komponente des Sicherheitsgateway-Systems nicht mit den VPN-Verbindungen belastet wird.
- Eine Freischaltung durch das ALG ist nicht erforderlich, so dass diese Lösung mit jedem ALG betrieben werden kann.
- Der entschlüsselte Datenverkehr kann durch den internen Paketfilter kontrolliert und eingeschränkt werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Es besteht prinzipiell eine Möglichkeit zur Umgehung des ALG über das Application-Level-Gateway. Diese ist in der Regel umso größer, je mehr Zusatzfunktionen die VPN-Komponenten über die VPN-Funktionalität hinaus anbieten.
- Der entschlüsselte Datenverkehr kann nicht auf Anwendungsebene kontrolliert und eingeschränkt werden, da die Verbindung mit dem ALG fehlt.

Empfehlung: Es wird zur Erzielung einer besonders hohen Sicherheit prinzipiell davon abgeraten, Netzkomponenten nach der in diesem Szenario beschriebenen Art parallel zum ALG zu schalten. Auch wenn es sich bei VPN-Gateways um Komponenten handelt, die nur einen sehr geringen Funktionsumfang besitzen und deshalb schwer anzugreifen sind, ist die Umgehungsmöglichkeit des ALG dennoch vorhanden. Diese ist bei SSL-VPNs höher als bei den anderen VPN-Technologien, da SSL-VPNs über die eigentliche VPN-Funktion hinaus noch weitergehende Funktionen besitzen, z. B. die Webifizierungsfunktion.

Eine Integration von VPN-Komponenten parallel zum ALG ist deshalb nicht zu empfehlen.

Die vorgestellte Lösung könnte dahingehend verändert werden, dass das VPN-Gateway nicht vor und hinter dem ALG mit dem Sicherheitsgateway verbunden wird, sondern an eine weitere Schnittstelle der beiden Paketfilter angeschlossen wird. In diesem Fall würde die VPN-Komponente stärker vom ALG getrennt und eine Übernahme des ALG bzw. der VPN-Komponente erschwert. Auch diese Variante wird, wie in Abschnitt 6.14.2 beschrieben, nicht empfohlen.

6.9 VPN-Komponente im Sicherheitsgateway integriert

Voraussetzung: Die VPN-Funktionalität muss im ALG integriert oder integrierbar sein. Der Einsatz von Zusatzprodukten wird von verschiedenen Produkten jedoch durch Sicherungsmaßnahmen auf dem ALG verhindert.

Vorteile:

- Durch die Integration der VPN-Funktionalität in das ALG wird die VPN-Komponente gegen Angriffe aus dem Internet geschützt.
- Aus dem Internet werden nur VPN-Verbindungen zum ALG zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Gängige Application-Level-Gateway-Produkte besitzen bereits die Funktionalität, VPN-Verbindungen über das nicht-vertrauenswürdige Netz zu betreiben. Dies kann eine günstige Alternative gegenüber separat zu installierenden VPN-Gateways sein.
- Eine Adressumsetzung der unverschlüsselten Pakete ist nicht erforderlich, da das ALG die Verbindungen selbst entschlüsselt und die entsprechenden Rückpakete in Richtung des nicht-vertrauenswürdigen Netzes auch wieder durch das ALG geroutet werden.
- Der entschlüsselte Datenverkehr kann durch den internen Paketfilter kontrolliert und eingeschränkt werden. Produktabhängig können entschlüsselte Verbindungen am ALG zusätzlich durch Proxies geleitet werden.

Nachteile:

- Der entschlüsselte Datenverkehr kann nicht auf Anwendungsebene kontrolliert und eingeschränkt werden, falls das verwendete Produkt nicht über entsprechende Konfigurationsmöglichkeiten verfügt.
- Die VPN-Funktionalität muss evtl. auf dem ALG integriert werden. Auch wenn die VPN-Funktionalität bereits vom Hersteller integriert wurde, stellt dies einen zusätzlichen Dienst auf dem ALG dar, der das Ziel von Angriffen sein kann und die Schutzfunktion des ALG kompromittieren könnte.
- Die Flexibilität bei der Wahl der VPN-Gegenstelle ist eingeschränkt, da das in das ALG integrierte VPN-Gateway im Falle von Inkompatibilitäten mit der VPN-Gegenstelle nicht ohne Weiteres gegen ein Alternativprodukt ausgetauscht werden kann. In der Regel muss hier ein dediziertes VPN-Gateway beschafft werden, das wie in Variante 6.11 beschrieben platziert werden muss, um eine ähnliche Funktion wie das in das ALG integrierte VPN-Gateway zu erzeugen.
- Bei starker Nutzung der VPN-Funktionalität kann die Performance des Application-Level-Gateways unter der erforderlichen Rechenleistung leiden, was zu Denial-of–Service der Netzanbindung führen kann.

Empfehlung: Aufgrund der vorhandenen Sicherheitsrisiken bei der Implementierung der VPN-Komponente auf dem ALG kann diese Realisierungsvariante nicht empfohlen werden.

6.10 Platzierung inline vor dem äußeren Paketfilter

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Da die VPN-Komponente inline platziert ist, kann diese eine implizite NAT-Funktion für das interne Netz bereitstellen.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Die VPN-Komponente steht ungeschützt im nicht-vertrauenswürdigen Netz und ist dadurch insbesondere auf Betriebssystemebene angreifbar. Dem kann nur durch Einsatz aktueller Softwareversionen, Härtung der Konfiguration und Deaktivierung aller nicht benötigten Dienste begegnet werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.
- Falls das VPN zur Absicherung des Zugriffs auf Systeme im vertrauenswürdigen Netz dient, muss der entschlüsselte Datenverkehr auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Somit sind umfangreiche Freischaltungen auf diesen Komponenten notwendig, da der entschlüsselte Verkehr möglicherweise viele Verbindungen umfasst. U. U. muss an dieser Stelle auch die Freischaltung bzw. Sperrung der Kommunikation für einzelne Rechner oder Server des vertrauenswürdigen Netzes erfolgen.
- Für den Fall, dass die Anbindung an das nicht-vertrauenswürdige Netz auch für Verbindungen genutzt werden soll, die unverschlüsselt betrieben werden, muss ein VPN-Produkt gewählt werden, das Verbindungen regelabhängig verschlüsselt oder transparent weiterleitet. Je nach vorliegenden Rahmenbedingungen ist zu diesem Zwecke auch eine Umgehung der VPN-Komponente denkbar.

Empfehlung: Aufgrund der fehlenden Schutzmöglichkeiten des VPN-Gateways und der erforderlichen Öffnung der kompletten Sicherheitsgateway-Struktur für eine Vielzahl von Protokollen wird die Aufstellung des VPN-Gateways vor dem externen Paketfilter nicht empfohlen.

6.11 Platzierung inline zwischen dem äußeren Paketfilter und dem ALG

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways hinter dem äußeren Paketfilter wird das System gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Da die VPN-Komponente inline platziert ist, kann diese eine implizite NAT-Funktion für das interne Netz bereitstellen.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Falls das VPN zur Absicherung des Zugriffs auf Systeme im vertrauenswürdigen Netz dient, muss der entschlüsselte Datenverkehr auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Somit sind umfangreiche Freischaltungen auf diesen Komponenten notwendig, da der entschlüsselte Verkehr möglicherweise viele Verbindungen umfasst. U. U.

muss an dieser Stelle auch die Freischaltung bzw. Sperrung der Kommunikation für einzelne Rechner oder Server des vertrauenswürdigen Netzes erfolgen.
- Für den Fall, dass die Anbindung an das nicht-vertrauenswürdige Netz auch für Verbindungen genutzt werden soll, die unverschlüsselt betrieben werden, muss ein VPN-Produkt gewählt werden, das Verbindungen regelabhängig verschlüsselt oder transparent weiterleitet. Je nach vorliegenden Rahmenbedingungen ist zu diesem Zwecke auch eine Umgehung der VPN-Komponente denkbar.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.

Empfehlung: Aufgrund der erforderlichen Öffnung des Application-Level-Gateways wird die Aufstellung des VPN-Gateways inline zwischen dem externen Paketfilter und dem ALG nicht empfohlen.

6.12 Platzierung inline zwischen dem ALG und dem internen Paketfilter

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways inline zwischen dem Application-Level-Gateway und dem internen Paketfilter wird das System durch den äußeren Paketfilter und das ALG gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Je nach Implementierung des ALG können VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz nur auf das ALG zugelassen werden. Das ALG leitet die Verbindungen dann zum VPN-Gateway weiter. Das VPN-Gateway, das mit dieser Methode keine offizielle IP-Adresse mehr braucht, ist somit nur für den VPN-Dienst erreichbar.
- Konfigurationsfehler des VPN-Gateways werden evtl. durch das ALG abgefangen, da dieses gegenüber dem nicht-vertrauenswürdigen Netz als Stellvertreter des VPN-Gateways auftritt.
- Bei einer LAN-LAN-VPN-Kopplung ist nur die Einrichtung eines Proxies für die VPN-Verbindung erforderlich. Die Einrichtung jeweils eines Proxies für die einzelnen Protokolle des unverschlüsselten Datenverkehrs ist nicht erforderlich.
- Da die VPN-Komponente inline platziert ist, kann diese eine implizite NAT-Funktion für das interne Netz bereitstellen.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Das ALG muss VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz direkt in das interne Netz weiterleiten, ohne die Inhalte der Verbindungen prüfen zu können.
- Der entschlüsselte Datenverkehr muss auf dem Weg in das vertrauenswürdige Netz nur noch den inneren Paketfilter passieren. Es ist keine Kontrolle der unverschlüsselten Verbindungen auf Anwendungsebene möglich.
- Für den Fall, dass die Anbindung an das nicht-vertrauenswürdige Netz auch für Verbindungen genutzt werden soll, die unverschlüsselt betrieben werden, muss ein VPN-Produkt gewählt werden, das Verbindungen regelabhängig verschlüsselt oder transparent weiterleitet. Je nach vorliegenden Rahmenbedingungen ist zu diesem Zwecke auch eine Umgehung der VPN-Komponente denkbar.
- Die Weiterleitung von VPN-Verbindungen durch das ALG kann produktspezifisch problematisch sein, z. B. ist es bei manchen ALGs nicht möglich, reines IPSec (ESP, AH) durchzulassen. In diesen Fällen ist zu prüfen, ob Ersatzlösungen, z. B. IPSec über UDP/500, möglich sind.

Empfehlung: Aufgrund der erforderlichen Freischaltung der VPN-Verbindungen von außen nach innen durch das Application-Level-Gateway wird die Platzierung der VPN-Komponente inline zwischen dem Application-Level-Gateway und dem internen Paketfilter nicht empfohlen.

6.13 Platzierung inline im internen Netz

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways im internen Netz wird das System durch beide Paketfilter und das ALG gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Je nach Implementierung des ALG können VPN-Verbindungen aus dem nicht-vertrauenswürdigen Netz nur auf das ALG zugelassen werden. Das ALG leitet die Verbindungen dann zum VPN-Gateway weiter. Das VPN-Gateway, das mit dieser Methode keine offizielle IP-Adresse mehr braucht, ist somit nur für den VPN-Dienst erreichbar.
- Konfigurationsfehler des VPN-Gateways werden evtl. durch das ALG abgefangen, da dieses gegenüber dem nicht-vertrauenswürdigen Netz als Stellvertreter des VPN-Gateways auftritt.
- Da die VPN-Komponente inline platziert ist, kann diese eine implizite NAT-Funktion für das interne Netz bereitstellen.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Das ALG und der interne Paketfilter müssen VPN-Verbindungen aus dem Internet direkt in das interne Netz weiterleiten, ohne die Inhalte der Verbindungen prüfen zu können.
- Der entschlüsselte Datenverkehr kann nicht mehr kontrolliert und eingeschränkt werden, so dass die VPN-Clients einen kompletten Zugriff auf das interne Netz erhalten.
- Für den Fall, dass die Anbindung an das nicht-vertrauenswürdige Netz auch für Verbindungen genutzt werden soll, die unverschlüsselt betrieben werden, muss ein VPN-Produkt gewählt werden, das Verbindungen regelabhängig verschlüsselt oder transparent weiterleitet.
- Die Weiterleitung von VPN-Verbindungen durch das ALG kann produktspezifisch problematisch sein, z. B. ist es bei manchen ALGs nicht möglich, reines IPSec (ESP, AH) durchzulassen. In diesen Fällen ist zu prüfen, ob Ersatzlösungen, z. B. IPSec über UDP/500, möglich sind.

Empfehlung: Aufgrund der erforderlichen Freischaltung der VPN-Verbindungen von außen nach innen durch das Application-Level-Gateway und der fehlenden Möglichkeiten zur Kontrolle der unverschlüsselten Verbindungen wird die Platzierung der VPN-Komponente inline zwischen dem internen Netz und dem internen Paketfilter nicht empfohlen.

6.14 Kombinationen

Speziell bei VPN-Produkten, die eine reine Gateway-Funktionalität mit einer internen und einer externen Schnittstelle implementieren, können sinnvolle Kombinationen der genannten Architekturen realisiert werden. Nachfolgend werden zwei Varianten besprochen, die eine Kombination der vorgenannten Architekturen realisieren.

6.14.1 VPN-Komponente am äußeren Paketfilter und ALG

Bei der ersten Kombinationsvariante wird das VPN-Gateway mit einer Netzschnittstelle am äußeren Paketfilter und mit der anderen Schnittstelle am ALG verbunden, wie in der nachfolgenden Abbildung dargestellt.

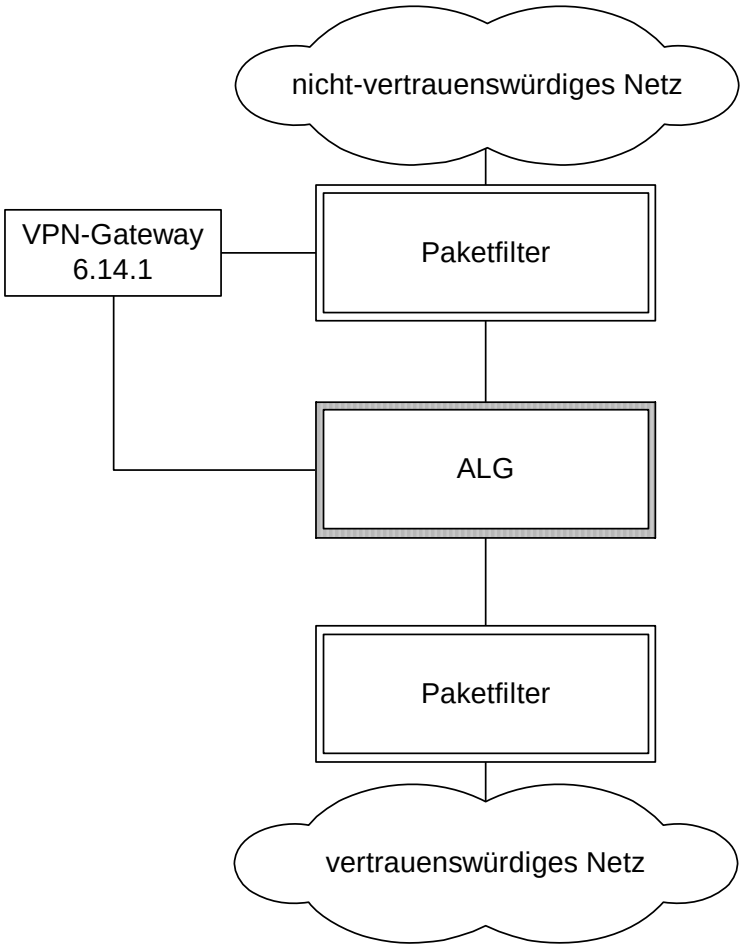


Abbildung 32 Anbindung des VPN-Gateways über eine getrennte Schnittstelle an das ALG

Voraussetzungen:

- Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.
- Der aus dem nicht-vertrauenswürdigen Netz eingehende, entschlüsselte Verkehr muss vom VPN-Gateway zum vertrauenswürdigen Netz über eine eigene Schnittstelle des ALG geleitet werden können (in die andere Richtung analog).

Vorteile:

- Durch die Platzierung des VPN-Gateways am äußeren Paketfilter wird die VPN-Komponente durch den äußeren Paketfilter gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Der entschlüsselte Datenverkehr kann auf Anwendungsebene kontrolliert und eingeschränkt werden, da die Verbindungen über das ALG geleitet werden.
- Die Gefahr von Konfigurationsfehlern wird dadurch verringert, dass das VPN-Gateway an ein dediziertes Interface des ALG angebunden wird. Insbesondere wenn über das VPN weitreichende Freischaltungen am ALG in das vertrauenswürdige Netz erforderlich sind, ist dieser Verkehr weniger fehlerträchtig vom Standardverkehr (z. B. HTTP, SMTP etc.) zu differenzieren.

- Der entschlüsselte Datenverkehr kann zusätzlich durch den internen Paketfilter kontrolliert und eingeschränkt werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.

Nachteile:

- Protokollierungsdaten, die vom VPN-Gateway generiert werden, müssen an das ALG gesendet und von einem Proxy in das interne Netz zum Loghost weitergeleitet werden. In den Protokolldateien erscheinen die Einträge dann mit der IP-Adresse des Proxies und lassen sich somit schwer von anderen Einträgen trennen, z. B., falls weitere Komponenten des Sicherheitsgateways ebenfalls Proxies des ALG zum Logging benutzen.
- Damit die Rückpakete der entschlüsselten Verbindungen wieder zum VPN-Gateway geleitet werden, muss eine Adressumsetzung verwendet werden.

Empfehlung: Die Platzierung des VPN-Gateways am externen Paketfilter und an eine separate Schnittstelle des Application-Level-Gateways kann empfohlen werden.

6.14.2 VPN-Komponente am äußeren und am inneren Paketfilter

Bei einigen Szenarien ist es nicht sinnvoll, den entschlüsselten Datenverkehr aus den VPN-Verbindungen auf Anwendungsebene zu prüfen und über das ALG zu leiten. In der Praxis wird man nur wenige der über VPN genutzten Dienste auf Anwendungsebene filtern können.

Daher ergeben sich weitere Platzierungvarianten, bei denen das interne Interface des VPN-Gateways nicht an das ALG, sondern an den inneren Paketfilter gebunden wird, ähnlich wie in Abschnitt 6.8.2 beschrieben:

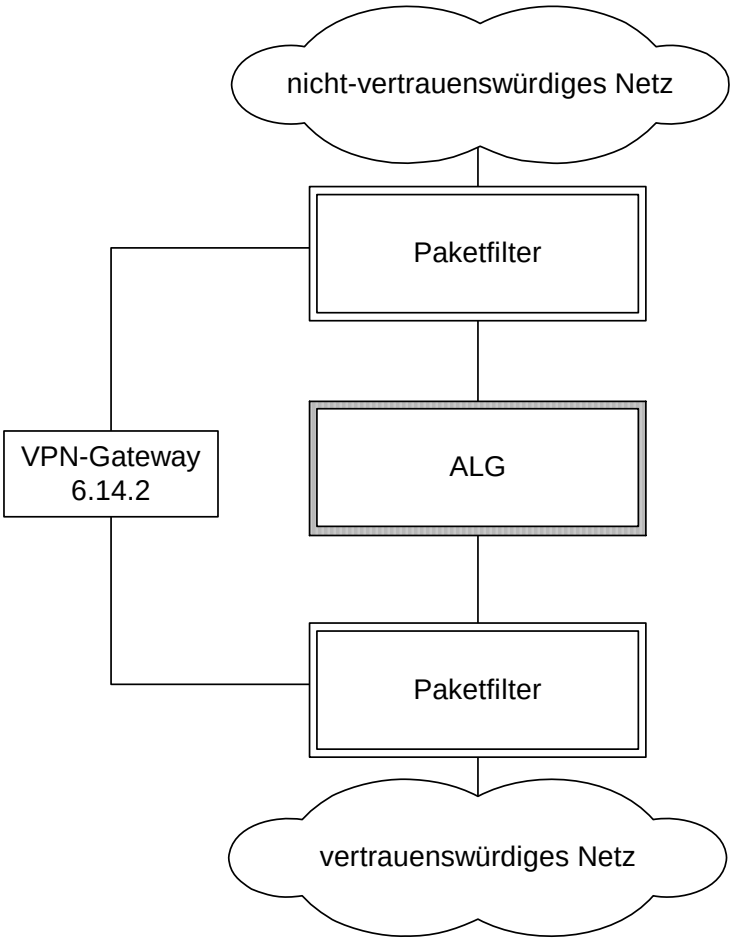


Abbildung 33 Anbindung des VPN-Gateways an die Paketfilter

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways am äußeren Paketfilter wird die VPN-Komponente gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.
- Die Lösung kann technisch fast in jedem Zusammenhang betrieben werden, da das ALG die Weiterleitung von VPN-Kommunikation nicht unterstützen muss.
- Der entschlüsselte Datenverkehr kann durch den internen Paketfilter kontrolliert und eingeschränkt werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können je nach Platzierung des Loghosts möglicherweise direkt zu diesem weitergeleitet werden.

Nachteile:

- Durch die Parallelschaltung des VPN-Gateways zum ALG besteht prinzipiell eine Möglichkeit zur Umgehung des ALG.
- Der entschlüsselte Datenverkehr kann nicht auf Anwendungsebene kontrolliert und eingeschränkt werden, da die Verbindungen nicht über das ALG geleitet werden.
- Werden entschlüsselte Pakete vom VPN-Gateway mit der original Client-IP-Adresse in das interne Netz weitergeleitet, muss sichergestellt werden, dass die Rückpakete der Verbindung

wieder zum VPN-Gateway gelangen. Dazu sind z. B. eine Adressumsetzung am VPN-Gateway oder Routing-Einstellungen im internen Netz notwendig.

Empfehlung: Es wird prinzipiell davon abgeraten, Netzkomponenten nach der in diesem Szenario beschriebenen Art parallel zum ALG zu schalten. Auch wenn es sich bei VPN-Gateways um Komponenten handelt, die nur einen sehr geringen Funktionsumfang besitzen und deshalb schwer anzugreifen sind, ist die Umgehungsmöglichkeit des ALG dennoch vorhanden. Diese ist bei SSL-VPNs in der Regel höher als bei den anderen VPN-Technologien, da SSL-VPNs über die eigentliche VPN-Funktion noch weitergehende Funktionen besitzen können, z. B. die Webbifizierungsfunktion.

Eine Integration von VPN-Komponenten als Umgehung des ALG ist deshalb nicht zu empfehlen.

6.14.3 VPN-Komponente am ALG und am inneren Paketfilter

Alternativ zu 6.14.2 kann die externe Netzschnittstelle des VPN-Gateways mit einer separaten Netzschnittstelle des ALG verbunden werden:

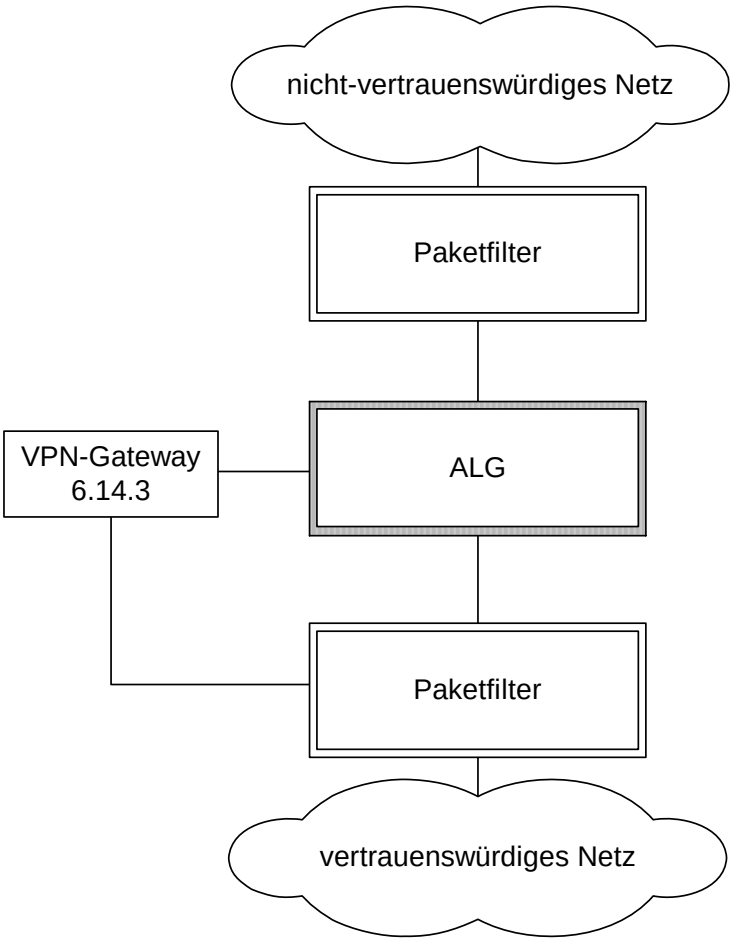


Abbildung 34 Anbindung des VPN-Gateways zwischen ALG und interner Paketfilter

Voraussetzung: Das VPN-Gateway muss mit zwei Netzschnittstellen betrieben werden können.

Vorteile:

- Durch die Platzierung des VPN-Gateways am ALG wird die VPN-Komponente gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt.
- Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind.

- Das ALG kann VPN-Verbindungen stellvertretend für das VPN-Gateway annehmen, so dass die VPN-Komponente nicht direkt aus dem nicht-vertrauenswürdigen Netz angesprochen wird. Die Verbindungen werden vom ALG zur VPN-Komponente weitergeleitet.
- Der entschlüsselte Datenverkehr kann durch den internen Paketfilter kontrolliert und eingeschränkt werden.
- Das VPN-Gateway kann aus dem internen Netz konfiguriert werden.
- Protokollierungsdaten, die vom VPN-Gateway generiert werden, können direkt in das interne Netz zum Loghost weitergeleitet werden.

Nachteile:

- Der entschlüsselte Datenverkehr kann nicht auf Anwendungsebene kontrolliert und eingeschränkt werden.
- Werden entschlüsselte Pakete vom VPN-Gateway mit der original Client-IP-Adresse in das interne Netz weitergeleitet, muss sichergestellt werden, dass die Rückpakete der Verbindung wieder zum VPN-Gateway gelangen. Dies ist z. B. durch eine Adressumsetzung am VPN-Gateway oder Routing-Einstellungen im internen Netz zu realisieren.

Empfehlung: Aufgrund der fehlenden Kontrollmöglichkeiten der unverschlüsselten Verbindungen auf Anwendungsebene kann die Platzierung des VPN-Gateways parallel zum Application-Level-Gateway nur für die Szenarien empfohlen werden, bei denen die Funktionalität des ALG nicht erforderlich ist. Dies ist dann der Fall, wenn das Client-System unter eigener Kontrolle steht oder die komplette TCP/IP-Bandbreite freigeschaltet werden muss. Hierbei handelt es sich um die folgenden Szenarien:

- mobiler Mitarbeiter
- Heimarbeitsplatz
- Standortvernetzung
- WLAN-Absicherung

6.15 Gegenüberstellung der Platzierungsvarianten

Zusammenfassend werden nachfolgend die Vor- und Nachteile der Architekturen tabellarisch gegenübergestellt.

Aufgrund der Unterschiede in den zu empfehlenden Platzierungsvarianten wurde die Übersicht nach Szenarien aufgeteilt. Die Kriterien sind als K.O.-Kriterien gekennzeichnet, wenn sie maßgebend für Empfehlung der Varianten sind.

Die jeweils empfohlenen Platzierungsvarianten sind grau hinterlegt.

In Tabelle 16 bis Tabelle 19 werden folgende Bezeichnungen verwendet:

x	erfüllt
-	nicht erfüllt
ePF	externer Paketfilter
iPF	interner Paketfilter

Tabelle 16: Vergleich der VPN-Varianten für Clients unter eigener Kontrolle

Variante **Kriterium**	**6.1** **vor ePF**	**6.2** **an ePF**	**6.3** **nach ePF**	**6.4** **an ALG**	**6.5** **nach ALG**	**6.6** **an iPF**	**6.7** **im LAN**
Schutz der VPN-Komponente gegen Angriffe (K.O.)	-	x	x	x	x	x	x
Kontrolle des VPN-Kanals (K.O.)	-	x	x	x	x	x	x
Kontrolle der unverschlüsselten Verbindungen (K.O.)	x	x	x	x	x	x	x
NAT erforderlich	x	x	x	x	x	x	x
Trennung auf Anwendungsebene (K.O.)	-	-	-	x	-	-	-
Keine zus. Dienste auf ALG (K.O.)	x	x	x	x	x	x	x
Erfüllung der Sicherheitsgrundfunktionen von VPN-Produkten (vgl. Kapitel 5.2)	Abhängig von der Produktauswahl für VPN und ALG						

Tabelle 17: Vergleich der VPN-Varianten für Clients unter eigener Kontrolle (Fortsetzung)

Variante **Kriterium**	**6.8.1 direkt**	**6.8.2 zwischen ePF u. iPF**	**6.9 im ALG integr.**	**6.10 inline vor ePF**	**6.11 inline ALG u. ePF**	**6.12 inline iPF u. ALG**	**6.13 inline im internen Netz**	**6.14.1 am ePF u. ALG**	**6.14.2 am ePF u. iPF**	**6.14.3 am ALG u. iPF**
Schutz der VPN-Komponente gegen Angriffe (K.O.)	-	x	x	x	-	x	x	x	x	x
Kontrolle des VPN-Kanals (K.O.)	-	x	x	x	-	x	x	x	x	x
Kontrolle der unverschlüsselten Verbindungen (K.O.)	-	x	x	x	-	x	x	x	x	x
NAT erforderlich	x	x	-	-	-	-	-	x	x	x
Trennung auf Anwendungsebene (K.O.)	-	-	x	-	-	-	x	x	-	-
Keine zus. Dienste auf ALG (K.O.)	x	x	-	x	x	x	-	x	x	x
Erfüllung der Sicherheitsgrund-funktionen von VPN-Produkten (vgl. Kapitel 5.2)	Abhängig von der Produktauswahl für VPN und ALG									

Tabelle 18: Vergleich der VPN-Varianten für Clients unter fremder Kontrolle

Variante **Kriterium**	**6.1** **vor ePF**	**6.2** **an ePF**	**6.3** **nach ePF**	**6.4** **an ALG**	**6.5** **nach ALG**	**6.6** **an iPF**	**6.7** **im LAN**
Schutz der VPN-Komponente gegen Angriffe (K.O.)	-	x	x	x	x	x	x
Kontrolle des VPN-Kanals (K.O.)	-	x	x	x	x	x	x
Kontrolle der unverschlüsselten Verbindungen (K.O.)	x	x	x	x	x	x	x
NAT erforderlich	x	x	x	x	x	x	x
Trennung auf Anwendungsebene (K.O.)	-	-	-	x	-	-	-
Keine zus. Dienste auf ALG (K.O.)	x	x	x	x	x	x	x
Erfüllung der Sicherheitsgrund-funktionen von VPN-Produkten (vgl. Kapitel 5.2)	Abhängig von der Produktauswahl für VPN und ALG						

Tabelle 19: Vergleich der VPN-Varianten für Clients unter fremder Kontrolle (Fortsetzung)

Variante **Kriterium**	**6.8.1 direkt**	**6.8.2 zwischen ePF u. iPF**	**6.9 im ALG integr.**	**6.10 inline vor ePF**	**6.11 inline ALG u. ePF**	**6.12 inline iPF u. ALG**	**6.13 inline im internen Netz**	**6.14.1 am ePF u. ALG**	**6.14.2 am ePF u. iPF**	**6.14.3 am ALG u. iPF**
Schutz der VPN-Komponente gegen Angriffe (K.O.)	-	x	x	x	-	x	x	x	x	x
Kontrolle des VPN-Kanals (K.O.)	-	x	x	x	-	x	x	x	x	x
Kontrolle der unverschlüsselten Verbindungen (K.O.)	-	x	x	x	-	x	x	x	x	x
NAT erforderlich	x	x	-	-	-	-	-	x	x	x
Trennung auf Anwendungsebene (K.O.)	-	-	x	-	-	-	x	x	-	-
Keine zus. Dienste auf ALG (K.O.)	x	x	-	x	x	x	x	x	x	x
Erfüllung der Sicherheitsgrund-funktionen von VPN-Produkten (vgl. Kapitel 5.2)	Abhängig von der Produktauswahl für VPN und ALG									

7. Empfehlungen zu Schutzmaßnahmen

Die nachfolgend beschriebenen Vorschläge zu Schutzmaßnahmen können als Basis für die Integration von VPN-Komponenten dienen und sind als Mindestanforderungen zu verstehen. Diese sind auf den entsprechenden Einsatzzweck und die gegebenen Rahmenbedingungen anzupassen. Speziell im Verschlusssachen-Bereich sind Anpassungen an den höheren Schutzbedarf notwendig und damit höhere Maßstäbe anzusetzen.

Zudem gilt: Wenn verbleibende Restrisiken für einen Dienst oder eine Dienstrichtung nicht tolerierbar sind, muss entweder auf die Nutzung der Anwendung oder einer Dienstrichtung verzichtet werden.

Die Schutzmaßnahmen werden in Abhängigkeit vom zu schützenden Objekt beschrieben:

- VPN-Kanal
  Maßnahmen zur Sicherung des VPN-Kanals. Relevant sind Maßnahmen zur Übertragungssicherung und zum Schlüsselmanagement. Identifikation, Authentisierung, Datenflusskontrolle und Beweissicherung können im VPN-Kanal nicht realisiert werden.
- Client-System, d. h. Tunnelendpunkt
  Maßnahmen zum Schutz des Clients, d. h. des Tunnel-Endpunktes. Hier sind Identifikation, Authentisierung, Datenflusskontrolle und Beweissicherung relevant.
- Interne Systeme, z. B. Server

Maßnahmen zum Schutz der Infrastruktur im vertrauenswürdigen Netz. Relevant sind Identifikation, Authentisierung, Datenflusskontrolle und Beweissicherung am Application-Level-Gateway. Krypto-Maßnahmen bieten keinen zusätzlichen Schutz, jedoch kann eine erfolgreich initiierte Verschlüsselung als Identifikation und Authentisierung mit einem Frage-Antwort-Verfahren eingestuft werden.

In den folgenden drei Unterkapiteln werden jeweils zu einem dieser drei Objekte Mindest-Schutzmaßnahmen empfohlen. Dabei wird die Anbindung von Tunnel-Endpunkten mit einer mittleren und hohen Vertrauenswürdigkeit betrachtet. Die Anbindung entfernter Endpunkte, die nur eine geringe Vertrauenswürdigkeit besitzen, wird nicht empfohlen. Deshalb werden für die Stufe „gering“ keine Empfehlungen angeboten.

7.1 Schutz des VPN-Kanals

In diesem Abschnitt wird vorgeschlagen, welche Schutzmaßnahmen für welche VPN-Verbindung bei der Absicherung des VPN-Kanals erforderlich sind:

VPN-Transferkanal **Vertrauenswürdigkeit des entfernten VPN-Tunnelendpunktes**	**Über ein nicht-vertrauenswürdiges (öffentliches) Netz**	**Über ein Netz unter eigener Kontrolle**
Hoch (dediziertes Gerät unter eigener Kontrolle)	Dienstunspezifische Verschlüsselung Statische Verteilung symmetrischer Hauptschlüssel und dynamische Verteilung symmetrischer Sitzungsschlüssel	Dienstunspezifische Verschlüsselung Statische Verteilung symmetrischer Schlüssel
Mittel (dediziertes Gerät unter fremder Kontrolle oder eigener/s PC/Notebook)	Dienstunspezifische Verschlüsselung Statische Verteilung symmetrischer Hauptschlüssel und dynamische Verteilung symmetrischer Sitzungsschlüssel	Dienstunspezifische Verschlüsselung Statische Verteilung symmetrischer Hauptschlüssel und dynamische Verteilung symmetrischer Sitzungsschlüssel

Tabelle 20: Schutz des VPN-Kanals

7.2 Schutz der Client-Systeme (Tunnel-Endpunkte)

Die Empfehlung zum Schutz der Client-Systeme lautet immer gleich, egal ob der VPN-Transferkanal über ein nicht-vertrauenswürdiges Netz oder über ein Netz unter eigener Kontrolle aufgebaut wird oder ob die Vertrauenswürdigkeit des entfernten VPN-Tunnelendpunktes “hoch” oder “mittel” ist.

Für alle Szenarien gilt also:

- Authentisierung mit konstanter Kennung zu Beginn. Vor Nutzung eines VPN-Kanals muss eine Authentisierung des Benutzers am verwendeten Rechner durch die Abfrage einer konstanten Kennung stattfinden.
- Maschinen- und dienstspezifische Kontrolle. Zum Schutz des für den VPN-Zugriff verwendeten Rechners wird eine Datenflusskontrolle auf Paketebene gefordert. Der Tunnelendpunkt ist durch einen Paketfilter abzusichern, der nur VPN-Verbindungen zulässt und alle anderen Verbindungsversuche abweist.
- Bezüglich der Beweissicherung gibt es keine Anforderungen an die Protokollierung.

7.3 Schutz der Infrastrukturen im vertrauenswürdigen Netz („interne Infrastruktur“)

In Tabelle 21 werden zur Absicherung von Zugriffen eines entfernten Systems oder Netzes auf Systeme und Daten im eigenen Netz Schutzmaßnahmen vorgeschlagen, in Abhängigkeit von der Vertrauenswürdigkeit des Übertragungsnetzes und des entfernten Tunnelendpunktes. Auch hier handelt es sich wieder um Mindestanforderungen, die auf den konkreten Einsatzfall angepasst werden müssen.

<table>
<tr><th>VPN-Transferkanal

Vertrauenswürdigkeit des entfernten VPN-Tunnelendpunktes</th><th>Über ein nicht-vertrauenswürdiges (öffentliches) Netz</th><th>Über ein Netz unter eigener Kontrolle</th></tr>
<tr><td>Hoch

(LAN unter eigener Kontrolle)</td><td rowspan="2">Die folgenden Anforderungen gelten gleichermaßen für die Vertrauenswürdigkeit “hoch” und “mittel” des entfernten Tunnelendpunktes.
Zugriffe nur nach einer eindeutigen Authentisierung lediglich zu Beginn einer Kommunikationsbeziehung, mindestens mittels Frage-Antwort-Verfahren, die für jede Authentisierung ein neues Passwort generieren. Aus abgehörten Authentisierungsdurchläufen dürfen keine zukünftigen Passwörter abgeleitet werden können. Die Authentisierung mittels Passwort ist unzureichend, da es im nicht-vertrauenswürdigen Netz abgehört und wiederverwendet werden könnte.
Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.
Der Datenfluss sollte minimal benutzerbezogen auf Anwendungsebene kontrolliert werden, wozu Appplication-Level-Gateways eingesetzt werden müssen. Zugriffe in das interne Netz sollten ausschließlich benutzerbezogen erfolgen.
Protokollierung aller ein- und ausgehenden Verbindungsversuche. Die Aufzeichnungen müssen aussagekräftig genug sein, um unberechtigten Zugang sicher zu erkennen und nachzuweisen. Mindestens folgende Daten sollen aufgezeichnet werden: Datum, Uhrzeit, Initiator des Ereignisses, Quelle, Ziel, Name des zu identifizierenden Subjekts oder Objekts, Erfolg bzw. Misserfolg des Versuchs.</td><td>Keine Funktionalitäten eines Sicherheitsgateways erforderlich, alle beteiligten Systeme/Netze stehen unter eigener Kontrolle (gleicher Schutzbedarf)</td></tr>
<tr><td>Mittel

(LAN unter fremder Kontrolle oder PC/Notebook)</td><td>Die Authentizität des Kommunikationspartners wird ausschließlich zu Beginn einer Kommunikationsbeziehung durch die Abfrage einer konstanten Kennung (z. B. eines Passworts) geprüft.
Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.
Die Datenflusskontolle erfolgt durch einen Paketfilter. Dieser lässt nur die auf den Servern zu veröffentlichenden Ports zu.
Protokollierung aller ein- und ausgehenden Verbindungsversuche. Die Aufzeichnungen müssen aussagekräftig genug sein, um unberechtigten Zugang sicher zu erkennen und nachzuweisen. Mindestens folgende Daten sollen aufgezeichnet werden: Datum, Uhrzeit, Initiator des Ereignisses, Quelle, Ziel, Name des zu identifizierenden Subjekts oder Objekts, Erfolg bzw. Misserfolg des Versuchs.
Handelt es sich bei dem entfernten Netz um eine Demilitarisierte Zone (DMZ) unter eigener Kontrolle, so können evtl. schwächere Sicherheitsmechanismen eingesetzt werden, wie z. B. die Identifikation ohne Überprüfung der Authentizität der Identifikationsinformationen.</td></tr>
</table>

Tabelle 21: Empfehlungen zum Schutz der internen Infrastruktur

8. Spezielle Funktionen von VPN-Komponenten

Bei der Entwicklung von VPN-Produkten gehen Hersteller unterschiedlichen Philosophien nach, die festlegen, unter welchen Rahmenbedingungen ein Produkt geeignet ist. Im Wesentlichen handelt es sich hierbei um die folgenden Faktoren:

- Möglichkeiten der Adressumsetzung
- Anzahl der Netzschnittstellen, mit denen das VPN-Gateway betrieben werden kann

Die Faktoren werden in den folgenden beiden Unterkapiteln behandelt.

8.1 Behandlung der Client-IP-Adressen

Ein zentrales Problem ist das Routing von IP-Paketen, falls Clients über VPN-Technologien in Netze eingebunden werden. Da die Clients in der Regel offizielle IP-Adressen verwenden, die zudem meist noch dynamisch vergeben werden, können Pakete mit solchen IP-Adressen oft nicht ohne Weiteres im internen Netz verwendet werden. Die folgenden drei Unterkapitel beschreiben die bestehenden Probleme und zeigen Lösungsmöglichkeiten auf.

8.1.1 Nutzung der Original-Client-Adressen im internen Netz

Werden entschlüsselte Pakete zunächst mit den IP-Adressen des Client-Systems in das interne Netz geleitet (z. B. bei IPSec im Tunnel-Mode), können die Router im internen Netz meist so konfiguriert werden, dass Routingentscheidungen anhand der IP-Adressen des Client-Systems getroffen werden und die Pakete zum Ziel gelangen.

Abhängig von der Platzierung des VPN-Gateways und der Produktauswahl kann diese Lösung zu Problemen führen, die in der Abbildung 35 verdeutlicht werden: Die zu einer VPN-Verbindung gehörenden Antwortpakete besitzen als Ziel-IP-Adresse die IP-Adresse des Clients. Falls das ALG eine Default-Route in das nicht-vertrauenswürdige Netz besitzt, werden die Antwortpakete nicht zum VPN-Gateway, sondern direkt zum Client-System gesendet.

Problematisch ist auch das Routing im internen Netz: Die Antwortpakete dieser Verbindungen müssen zum VPN-Gateway zurückgeroutet werden. Dies ist nur möglich, wenn die Client-Adressen aus einem definierten Adressenpool stammen und diese Adressen nicht im internen LAN verwendet werden.

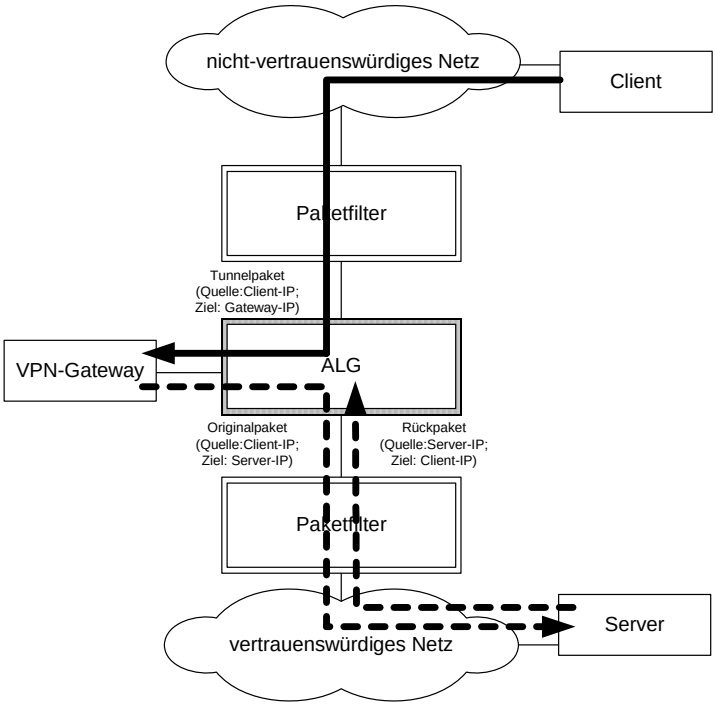


Abbildung 35 Routing-Problematik

Wenn die Client-Adressen dynamisch vergeben werden, verbleibt nur die Möglichkeit, die Default-Route auf das VPN-Gateway zu legen. Falls die Default-Route auch für sonstige Dienste erforderlich ist (z. B. HTTP), muss das VPN-Gateway im Application-Level-Gateway integriert werden, oder es muss sich um ein Inline-VPN-Gateway handeln.

Die in den beiden folgenden Unterkapiteln beschriebenen Lösungen beseitigen die eben beschriebenen Probleme.

8.1.2 Temporärer Austausch der Client-Adressen durch die Adresse des VPN-Gateways

Das VPN-Gateway ersetzt die ursprüngliche Client-IP-Adresse durch die IP-Adresse des VPN-Gateways. Alle Antwortpakete werden hierdurch zum VPN-Gateway geroutet, das die ursprüngliche Client-Adresse wieder einsetzt, so dass das Paket über den VPN-Tunnel zum Client weitergeleitet werden kann.

Im internen Netz können die Clients damit nicht mehr anhand der IP-Adresse differenziert werden, da jedes Paket als Absenderadresse die IP-Adresse des VPN-Gateways besitzt. Es ist somit kaum eine detaillierte Sperrung auf TCP/IP-Ebene mehr möglich, im Prinzip müssen alle Verbindungen, die vom VPN-Gateway nach innen initiiert werden, erlaubt werden.

Die Funktion der Adressenersetzung wird implizit erreicht, indem der über das nicht-vertrauenswürdige Netz eingehende VPN-Tunnel am VPN-Gateway terminiert und vom VPN-Gateway eine neue VPN-Verbindung in das interne Netz initiiert wird, das VPN-Gateway also als “VPN-Proxy” agiert. Auch bei dieser Lösung werden die IP-Adressen der Clients durch IP-Adressen des VPN-Gateways ersetzt.

8.1.3 Temporärer Austausch der Client-Adressen durch beliebige IP-Adressen

Im Unterschied zur Variante aus dem Kapitel 8.1.2 wird das VPN-Gateway hier so konfiguriert, dass es jedem VPN-Client eine eigene IP-Adresse zuweist und nicht jedem Client die Adresse des VPN-Gateways. Somit ist bekannt, welche IP-Adresse zu welchem Client gehört, und es können detaillierte Filterregeln eingesetzt werden.

In diesem Fall können die IP-Adressen so gewählt werden, dass sie zum Routing im internen Netz passen.

Der temporäre Austausch der Client-Adressen durch beliebige IP-Adressen wird nicht von allen VPN-Produkten unterstützt.

8.2 Anzahl der Schnittstellen am VPN-Gateway

Einige VPN-Produkte arbeiten ausschließlich mit zwei Schnittstellen, die als interne bzw. externe Schnittstelle konfiguriert werden müssen. Diese Systeme besitzen eine reine Gateway-Funktionalität und können wie folgt integriert werden:

Jede Schnittstelle wird in einem unterschiedlichen Netz betrieben. Das VPN-Gateway wird z. B. wie unter Abschnitt 6.10 beschrieben integriert.

Beide Schnittstellen werden an einem Switch/Router/Hub angeschlossen, erhalten aber jeweils IP-Adressen aus unterschiedlichen Netzsegmenten. Voraussetzung ist, dass im physikalisch gleichen Netz die Definition mehrerer IP-Netze oder VLANs möglich ist. Bei VLANs ist zu beachten, dass diese aufgrund möglicher Angriffe zurzeit noch nicht zu Sicherheitszwecken eingesetzt werden sollten.

9. Ausbauformen von VPN-Gateways

VPN-Gateways sind bzgl. der verwendeten Hard-/Software in verschiedenen Ausprägungen verfügbar. Einige Grundtypen und Ratschläge zur sicheren Verwendung werden in den folgenden Unterkapiteln vorgestellt.

9.1 Dedizierte VPN-Gateways

Dedizierte VPN-Produkte dienen ausschließlich der Realisierung von VPN-Verbindungen und bieten keine darüber hinausgehenden Funktionalitäten, wie z. B. die Inhaltsfilterung auf Anwendungsebene. Diese Produkte lassen sich meist auf handelsüblichen PC-Systemen mit Standard-Betriebssystemen installieren, sind aber auch als Fertigprodukte („Appliances“) erhältlich, die eine Hard-/Softwarekombination darstellen.

Fertigprodukte bieten den Vorteil, dass sie oft bereits für den VPN-Einsatz optimiert sind und einfach konfiguriert werden können. Wird Software auf einem Standard-Betriebssystem installiert, müssen häufig noch Dienste des Betriebssystems deaktiviert oder der Betriebssystemkern neu übersetzt werden – eine Fehlkonfiguration wird somit wahrscheinlicher. Bei Selbstinstallation wird der Einsatz eines Paketfilters empfohlen, um die VPN-Komponente abzusichern.

9.2 “Kombi-Geräte”

Kombi-VPN-Geräte sind beispielsweise Router oder andere Netzkomponenten, die neben ihrer eigentlichen Aufgabe auch eine VPN-Funktionalität bieten oder entsprechend erweitert werden können.

Die Kombination verschiedener Funktionalitäten auf einem Gerät kann zu Lasten der Performance gehen. Bei einer intensiven VPN-Nutzung ist daher die Verwendung eigenständiger VPN-Komponenten zu empfehlen.

9.3 Eigenbau

VPN-Geräte können mit frei verfügbaren Softwarekomponenten selbst zusammengestellt werden. Diese Komponenten können oft auf handelsüblicher Hardware mit Standardbetriebssystemen installiert werden. Zusammengestellte VPN-Geräte sind für kleine und mittlere Organisationen prinzipiell geeignet und können bei der Beschaffung erhebliche Kosteneinsparungen erbringen, da frei verfügbare Software in der Regel kostenlos ist.

Die Installation und Integration der frei verfügbaren Software ist fehlerträchtig, so dass sich erhebliche Sicherheitseinbußen ergeben können. Dem können spezielle VPN-Distributionen entgegenwirken, die auf diesen Einsatzzweck auch betriebssystemseitig zugeschnitten sind.

Support-Teams wie bei kommerziellen Produkten können meist nicht in Anspruch genommen werden. Das Know-How liegt oft bei den Entwicklern.

Zusammengestellte VPN-Geräte können daher für den Einsatz vor allem in größeren Organisationen nicht empfohlen werden.

9.4 Gegenüberstellung der Ausbauformen

Zusammenfassend werden nachfolgend die Vor- und Nachteile der unterschiedlichen Ausbauformen tabellarisch gegenübergestellt. Es handelt sich um eine grobe Einschätzung, produktspezifisch kann die Bewertung variieren.

Die Produktarten, die für den Einsatz als VPN-Gateway empfohlen werden, sind in Tabelle 22 grau hinterlegt.

Tabelle 22: Vergleich der VPN-Varianten (“x” = erfüllt, “-“ = nicht erfüllt)

Eigenschaft	Dediziert	Kombiniert	Eigenbau
(Selbst-)Schutz der VPN-Komponente	-	x	-
hohe Performance	x	-	x
günstige Anschaffungskosten	-	-	x
geringer Aufwand bis zur Inbetriebnahme	x	x	-
einfache Administration	x	x	-
leichte Erweiterbarkeit	-	-	x
Know-how-Verteilung	x	x	-
Support vom Hersteller	x	x	-

10. Wahl der Krypto-Varianten und Authentisierungsmechanismen

Bei der Realisierung eines VPN stehen verschiedene Krypto-Varianten zur Auswahl, die für unterschiedliche Anwendungen geeignet sind. Diese Varianten wurden in Abschnitt 4 detailliert beschrieben. Nachfolgend wird vereinfacht dargestellt, welche Technik für welche Anwendung bzw. für welches Szenario geeignet erscheint und welche Authentisierungsmechanismen für die einzelnen Szenarien empfohlen werden können. Auch hier wird wieder angemerkt, dass es je nach Rahmenbedingungen sinnvoll sein kann, von diesen Vorschlägen abzuweichen.

Tabelle 23: Empfehlungen für die Krypto-Varianten und Authentisierungsmechanismen

Anwendung	Krypto-Variante	Authentisierung	Szenario
Kopplung von LANs über nicht-vertrauenswürdige Netze	IPSec	Maschinenbezogene Authentisierung: • Zertifikate, SmartCards ohne PIN • Shared Secret	Heimarbeitsplatz Standortvernetzung Anbindung von Kunden und Partnern Fernwartung
Zugriffe von Client-Systemen, die unter eigener Kontrolle stehen	IPSec	Personenbezogene Authentisierung: • PKI vorhanden: Zertifikate, SmartCards mit PIN • Einmal-Passwörter • Shared Secret, Nutzername/Passwort (geschützt zu übertragen)	Mobiler Mitarbeiter Heimarbeitsplatz WLAN-Absicherung Fernwartung
Nutzung und Absicherung von wenigen Anwendungen Zugriffe über Terminalserver (Web-fähig)	SSL-VPN	Personen- und anwendungsbezogene Authentisierung: • Falls PKI vorhanden: Zertifikate, SmartCards mit PIN • Einmal-Passwörter • Shared Secret, Nutzername/Passwort (geschützt zu übertragen)	Mobiler Mitarbeiter Anbindung von Kunden und Partnern Fernwartung
Zugriffe von fremden	SSL-VPN	Personenbezogene Authentisierung:	Anbindung von Kunden

Anwendung	Krypto-Variante	Authentisierung	Szenario
Systemen, die nicht unter eigener Kontrolle stehen		• Falls SmartCard-Lesegerät und PKI vorhanden: SmartCards mit PIN • Einmal-Passwörter • Shared Secret, Nutzername/Passwort (geschützt zu übertragen)	und Partnern
Zugriffe von fremden Systemen, die nicht unter eigener Kontrolle stehen, jedoch bekannt sind	IPSec	Personen- und maschinenbezogene Authentisierung: • Falls PKI vorhanden: Zertifikate, SmartCards mit PIN • Einmal-Passwörter • Shared Secret, Nutzername/Passwort (geschützt zu übertragen)	Fernwartung durch Fremdfirmen
Tunneling von Broad- und Multicasts, Übertragung von Nicht-IP-Protokollen	L2TP SSL-VPN (Bridging)	Maschinenbezogene Authentisierung: • Zertifikate, SmartCards ohne PIN • Shared Secret	Heimarbeitsplatz Standortvernetzung

Anm.: Einmal-Passwörter sind problematisch bei häufigen ungewollten Verbindungsabbrüchen wie evtl. bei WLAN, GPRS, UMTS etc., da für jede Verbindung das Einmal-Passwort neu eingegeben werden muss. Einmal-Passwörter sind zudem nicht praktikabel bei einer hohen Anzahl von Clients.

Anhang

Anlage 1 Checklisten

Im Folgenden werden Funktionalitäten von VPN-Komponenten aufgelistet, die bei einer Beschaffung relevant sein könnten. Die Liste soll verhindern, dass falsche Produkte beschafft werden, weil einzelne Anforderungen übersehen wurden und von der beschafften Komponente nicht unterstützt werden.

Die folgenden Anforderungen sind grundlegender Art, d. h., sie dürften von vielen derzeit verfügbaren, professionellen Komponenten erfüllt werden und in vielen Einsatzumgebungen zutreffend sein. Neben den allgemeinen Anforderungen sind jedoch unbedingt noch die speziellen Anforderungen einzubeziehen, die sich z. B. aus den speziellen Einsatzbedingungen, der Kommunikationstopologie, den Diensten und Geräten ergeben. Eine Betrachtung der Anforderungen im Einzelfall ist unerlässlich. Nur so kann eine sinnvolle Produktentscheidung getroffen werden, die Voraussetzung für ein akzeptables Maß an Sicherheit ist.

Es muss also einerseits davon ausgegangen werden, dass die allgemeinen Anforderungen in den speziellen Einsatzumgebungen nicht ausreichen. Andererseits ist es auch möglich, dass einzelne Anforderungen im Einzelfall nicht erfüllt werden müssen, da hier die Anforderungen neu gewichtet werden.

Anforderung		**relevant**	**erfüllt**	
			ja	**nein**
Authentifizierung auf Maschinenebene				
Authentifizierung auf Anwendungs-/Benutzerebene				
Unterstützung unterschiedlicher Authentifizierungsverfahren				
Erweiterung um weitere Authentifizierungsverfahren				
Authentifizierung über einen RADIUS-Server				
Authentifizierung über einen externen Zertifikats-Server				
Authentifizierung über einen eingebauten Zertifikats-Server				
Protokollierung bzgl. des Detaillierungsgrades konfigurierbar				
Protokollierung von	Datum			
	Uhrzeit			
	Benutzer-ID des Initiators			
	Name des Kommunikationspartners (Rechner, Prozess oder Benutzer)			

Anforderung		relevant	erfüllt	
			ja	nein
	Verbindungsparameter			
	Name des zu identifizierenden Subjekts oder Objekts			
	Erfolg oder Misserfolg des Verbindungsversuchs			
	Aufzeichnung für jede eingehende Verbindung			
	Aufzeichnung für jede ausgehende Verbindung			
Verschlüsselung auf Maschinenebene				
Verschlüsselung auf Anwendungsebene				
Restriktion des Zugriffs auf das VPN mittels	Datum			
	Uhrzeit			
	Benutzer			
	Status des Virenscanners			
	Status der Personal Firewall			
	Aktualität der Patchinstallation			
Gleichzeitiges Weiterleiten von verschlüsseltem und unverschlüsseltem Verkehr				
Integrierter Packet-Sniffer zum Mitschneiden sowohl verschlüsselter als auch unverschlüsselter Pakete				
Weiterleitung der Protokolle	Sun Remote Procedure Call (RPC)			
	Microsoft Remote Procedure Call (RPC)			
	Voice Over IP			
	UDP			
Erzeugung von VLANs möglich				
Realisierung der in Abschnitt 7.1 geforderten Krypto- und Authentisierungsmechanismen				
Betrieb unterschiedlicher Tunnel mit unterschiedlichen Parametern				
Betrieb mit einer Netzschnittstelle möglich				
Betrieb mit zwei Netzschnittstellen möglich				
Erweiterung um Netzschnittstellen möglich				
Redundanter Betrieb möglich (Hot- oder Cold-Standby)				

Anforderung	relevant	erfüllt	
		ja	nein
Automatisches Fail-Over im Falle eines Ausfalls möglich			
Ausschließlich verschlüsselte Speicherung aller zu einer VPN-Session gehördenden Informationen (z. B. Authentisierungsinformationen, gewählte Schlüsselverfahren, Schlüssel)			
Sowohl bei beabsichtigter als auch unbeabsichtigter Beendigung des VPNs: Löschen aller zwischengespeicherten Informationen, die den Wiederaufbau eines VPN ermöglichen können.			
Nach einem Reboot: Löschen aller zwischengespeicherten Informationen, die den Aufbau eines VPN ermöglichen können.			
Konfigurationsmöglichkeit, um Pakete auf dem Rückweg zum VPN-Gateway leiten zu können (bei NAT oder Proxy-Funktionalität, siehe auch Abschnitt 8.1)			
Konfigurationsmöglichkeit, um bei der Adressumsetzung den VPN-Clients separate interne Adressen zuweisen zu können			
Möglichkeit zur temporären Entschlüsselung, um den gesamten Netzverkehr auf Schadprogramme filtern zu können			
VPN-Betrieb ist möglich, ohne dass aktive Inhalte von den Clients heruntergeladen werden müssen. Aktive Inhalte müssen dann im Browser nicht aktiviert werden.			

Tabelle 24: Checkliste für die Produktauswahl

Anlage 2 Relevante VPN-Standards und -Drafts

Nummer	Titel	Datum
RFC3686	Using Advanced Encryption Standard (AES) Counter Mode With IPSec Encapsulating Security Payload (ESP)	Januar 2004
RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPSec	September 2003
RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec	September 2003
RFC2857	The Use of HMAC-RIPEMD-160-96 within ESP and AH	Juni 2000
RFC2451	The ESP CBC-Mode Cipher Algorithms	November 1998
RFC2410	The NULL Encryption Algorithm and Its Use With IPSec	November 1998
RFC2409	The Internet Key Exchange (IKE)	November 1998
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)	November 1998
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP	November 1998
RFC2406	IP Encapsulating Security Payload (ESP)	November 1998
RFC2402	IP Authentication Header	November 1998
RFC2401	Security Architecture for the Internet Protocol	November 1998
RFC2637	Point-to-Point Tunneling Protocol (PPTP)	Juli 1999
RFC2661	Layer Two Tunneling Protocol (L2TP)	August 1999
RFC2246	The TLS Protocol Version 1.0	Januar 1999
RFC2631	Diffie-Hellman Key Agreement Method	Juni 1999

Anlage 3 Abkürzungen, Glossar

ALG	Application-Level-Gateway
BSI	Bundesamt für Sicherheit in der Informationstechnik
DMZ	Demilitarisierte Zone
FTP	File Transfer Protocol
HMAC	Hashed message authentication code
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
IT	Informationstechnik
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
OTP	One Time Password
PKI	Public Key Infrastructure
PPP	Point-To-Point Protocol
PPTP	Point-To-Point Tunneling Protocol
RAS	Remote Access
SA	Security Assocation
SAD	Security Association Database
SMTP	Simple Mail Transfer Protocol
SPD	Security Policy Database
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TELNET	Terminal Network
TLS	Transport Layer Security
UDP	User Datagram Protocol

UNIX	Uniplexed Information and Computing System
VPN	Virtual Private Network
WWW	World Wide Web

Kryptoanalyse

Kryptoanalyse ist ein Teilgebiet der Kryptologie. Das Ziel der Kryptoanalyse ist es, Informationen aus verschlüsselten Nachrichten zu gewinnen. Diese Informationen können die beteiligten Schlüssel oder die Nachricht selbst betreffen.

Kryptologie

Die Kryptologie beschäftigt sich mit der Ver- und Entschlüsselung von Informationen.

Nonce

In diesem Dokument wird der Begriff „Nonce“ für eine pseudo-zufällige, einmalig zu benutzende Bitfolge verwendet.

Perfect Forward Secrecy (PFS)

Der Begriff Perfect Forward Secrecy (PFS) bezeichnet eine Eigenschaft von Sitzungsschlüsseln, falls diese aus kompromittierten Sitzungs- oder Authentisierungsschlüsseln bereits ausgetauschter Nachrichten nicht mit vertretbarem Aufwand abgeleitet werden können.

In der Praxis wird PFS durch die Ausführung eines Diffie-Hellman-Austauschs für jeden neuen Sitzungsschlüssel realisiert.

Security Association (SA)

Unter Security Association (SA) versteht man eine Beziehung zwischen zwei oder mehr Entitäten, welche diesen erlaubt, sicher miteinander zu kommunizieren. Diese Beziehung charakterisiert die zum Schutz der ausgetauschten Daten benutzten Verfahren und deren Parameter.

Anlage 4 Kryptografische Grundlagen

In den folgenden Abschnitten werden die für VPNs relevanten kryptographischen Grundlagen skizziert. Vertiefende Informationen sind z. B. im IT-Grundschutzhandbuch des BSI zu finden (http://www.bsi.bund.de/gshb/deutsch/m/m03023.html). Ein sehr umfangreiches Glossar der IT-Sicherheit wird vom IETF als RFC 2828 bereitgestellt.

Anlage 4.1 Kryptographische Hash-Algorithmen

Mit Hash-Algorithmen kann jeder Nachricht ein Wert fester Bitlänge zugeordnet werden. Sie zeichnen sich dadurch aus, dass kleinste Veränderungen der Nachricht Änderungen des Hash-Werts hervorrufen.

Ein kryptographischer Hash-Algorithmus gilt als sicher, wenn es extrem aufwändig ist, aus dem Hash-Wert auf eine passende Nachricht zu schließen und gezielt Kollisionen, d. h. zwei Nachrichten mit den gleichen Hash-Werten, zu finden.

In der VPN-Praxis haben die in Tabelle 25 zusammengefassten Hash-Algorithmen eine große Bedeutung.

Abkürzung	Name	Hash-Wert-Länge	VPN-Verwendung
MD5	Message Digest 5	128 bit	IPSec, SSL
SHA-1	Secure Hash Algorithm	160 bit	IPSec, SSL, PPTP
SHA-2	Secure Hash Algorithm	256, 386, 512 bit	IPSec[1]
RIPEMD-160	RACE Integrity Primitives Evaluation Message Digest	160 bit	IPSec[2]

Tabelle 25: Hash-Algorithmen in VPN-Implementationen

Erläuterungen zur Tabelle:

[1] Obwohl nicht standardisiert, wird SHA-2 bereits in IPSec-Implementierungen vereinzelt eingesetzt.

[2] Als Erweiterung zu IPSec (RFC 2857).

Im August 2004 wurde die Sicherheit von MD5 bei der Verwendung in Zertifikaten und bei der Signierung in Frage gestellt, da Kollisionen gefundenen wurden (Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu, http://eprint.iacr.org/2004/199.pdf). Bislang ist aber noch unklar, ob die gefundenen Schwächen zu erfolgreichen Angriffen genutzt werden können.

Für die Verwendung von MD5 in HMAC-Verfahren (in IPSec und SSL) zur Sicherung der Integrität und Authentizität der ausgetauschten Daten ist diese Schwäche nicht relevant.

Die Angriffe auf SHA-0 konnten bislang lediglich auf SHA-1 mit reduzierter Rundenzahl erfolgreich angewandt werden. Die Benutzung von SHA-1 sollte jedoch laut Empfehlungen von National Institute of Standards and Technology (NIST) bis 2010 eingestellt werden (http://csrc.nist.gov/hash_standards_comments.pdf).

Anlage 4.2 Symmetrische Verschlüsselung

Bei symmetrischen Verschlüsselungsverfahren wird der gleiche Schlüssel für Ver- und Entschlüsselung verwendet. Es wird dabei zwischen Block- und Stromchiffren unterschieden. Diese werden in den folgenden Abschnitten diskutiert.

Anlage 4.1.2 Blockchiffren

Eine Blockchiffre unterteilt die zu verschlüsselnde Nachricht in Blöcke und führt die Verschlüsselung meist in mehreren Runden an ganzen Blöcken durch. Damit die Verschlüsselung von gleichen Klartext-Blöcken keine gleichen Ergebnisse liefert, werden bei den meisten Implementierungen sogenannte „Modes of operations“ benutzt. Damit hängt die Verschlüsselung nicht nur vom Klartext und vom Schlüssel ab, sondern zusätzlich vom vorhergehenden Verschlüsselungsblock oder vorhergehenden Klartextblock. Einige bekannte Modi sind der „Cipher Block Chaining Mode“ (CBC Mode), der „Cipher Feedback Mode“ (CFB Mode) und der „Output Feedback Mode“ (OFB Mode).

Tabelle 26 gibt einen Überblick über die wichtigsten Blockchiffren.

Abkürzung	Vollst. Name / weitere Bezeichnungen	Schlüssellänge	Blocklänge	Runden	VPN-Verwendung
AES	Advanced Encryption Standard (Rijndael)	128, 192, 256 bit	128 bit	10, 12, 14	IPSec[1], SSL[2]
DES	Data Encryption Algorithm	40, 56 bit	64 bit	16	IPSec, SSL
3DES	Triple DES	112	64 bit	3 * 16	IPSec, SSL
-	Blowfish	32-448 bit[3]	64 bit	16	IPSec
CAST	Auch CAST5 oder CAST-128	40-128 bit[3]	64 bit	12, 16	IPSec
IDEA	International Data Encryption Algorithm	128 bit	64 bit	8, 5	IPSec, SSL
RC2	Rivest Cipher 2	variabel	64 bit	18	SSL
RC5	Rivest Cipher 5	32, 64, 128 bit	1- 2040 bit	1- 255	IPSec

Tabelle 26: Wichtigste Blockchiffren

Anlage 4.2.2 Stromchiffren

Erläuterungen zur Tabelle:

[1] Als Erweiterung zu IPSec (RFC 3566, RFC 3602 und RFC 3686).

[2] Als Erweiterung zu TLS 1.0 (RFC 3268).

[3] In 8-Bit-Schritten.

In der Stromchiffrierung wird aus dem Schlüssel ein Bitstrom erzeugt, welcher bitweise mit der Nachricht verknüpft wird, z. B. mit dem logischen XOR. Diese Chiffren sind oft bei Weitem effizienter als Blockchiffren und werden vor allem in Geräten mit nur geringer Rechenkraft eingesetzt.

Es hat sich allerdings in der Vergangenheit gezeigt, dass Stromchiffren häufig anfälliger gegen Kryptoanalyse sind. Auch weil in der heutigen Zeit die Rechenkraft der meisten Geräte für Blockchiffren ausreichend ist, werden Stromchiffren im sensiblen Umfeld immer mehr durch Blockchiffren ersetzt.

Die bekannteste und am meisten verbreitete Stromchiffre ist der Rivest Cipher 4 (RC4). Im VPN-Umfeld wird RC4 in PPTP, SSL und (selten) in IPSec-Implementierungen verwendet. RC4 wird zwar als Verschlüsselungsalgorithmus für ESP in RFC 2407 vorgesehen, seine genaue Implementierung wurde jedoch nicht als Standard veröffentlicht.

Es sind Schwächen von RC4-Implementierungen bekannt, beispielsweise die Schwächen der WEP-Verschlüsselung im WLAN-Standard IEEE 802.11. Die Sicherheit des Algorithmus wird oft auf theoretischer Ebene in Frage gestellt (http://en.wikipedia.org/wiki/RC4#Security). Die SSL-Implementierung von RC4 ist laut RSA Laboratories von diesen Schwächen nicht betroffen (http://www.rsasecurity.com/rsalabs/node.asp?id=2009), die Überprüfung anderer Implementierungen wird jedoch empfohlen.

Andere Stromchiffren werden in dem hier behandelten VPN-Umfeld nicht verwendet.

Anlage 4.3 Asymmetrische Verschlüsselung: Public-Key-Verschlüsselung/Signierung

In asymmetrischen Verschlüsselungsverfahren wird statt eines einzigen Schlüssels ein Schlüsselpaar verwendet, bestehend aus einem so genannten öffentlichen Schlüssel („Public Key“) und einem geheimen Schlüssel („Secret“ oder „Private key“). Daten, die mit dem öffentlichen Schlüssel des Paares verschlüsselt wurden, können nur mit dem geheimen Schlüssel desselben Paares entschlüsselt werden. Die Schlüssel des Schlüsselpaares sind mathematisch miteinander verknüpft, können jedoch nicht mit vertretbarem Aufwand voneinander abgeleitet werden.

Die Schlüsselpaare sind nicht an Kommunikationskanäle, sondern an die kommunizierenden Entitäten (z. B. Rechnersysteme, natürliche Personen) gebunden. Der öffentliche Schlüssel wird bekannt gegeben. Der geheime Schlüssel verbleibt bei der Entität.

Will A eine sichere Nachricht für B versenden, so verschlüsselt A diese Nachricht mit dem öffentlichen Schlüssel von B. Nach Erhalt der verschlüsselten Nachricht kann B diese unter Verwendung seines privaten Schlüssels entschlüsseln.

Eine zweite Anwendung von asymmetrischen Verfahren ist die so genannte elektronische Signatur. Will A die Authentizität und Integrität seiner Nachricht sichern, signiert A diese Nachricht mit seinem privaten Schlüssel. Kann B mit Hilfe des öffentlichen Schlüssels von A die Signatur der Nachricht verifizieren, so ist es gewährleistet, dass diese mit dem privaten Schlüssel von A signiert wurde.

Bei der Signierung z. B. mittels des RSA-Verfahrens wird der Hashwert einer Nachricht mit dem privaten Schlüssel von A verschlüsselt und mit der Nachricht an B versendet. Der Kommunikationspartner kann den Hashwert selbst ermitteln und diesen mit dem Ergebnis der Entschlüsselung vergleichen.

Die Sicherheit der Verschlüsselung und der Signierung hängen im Wesentlichen von der Sicherheit des privaten Schlüssels ab. Den besten Schutz bietet die Erzeugung des Schlüsselpaares auf einer SmartCard. In diesem Fall verbleibt der private Schlüssel auf der SmartCard und kann nicht ausgelesen oder kopiert werden.

Ein weiteres Problem ist die sichere Zuordnung eines öffentlichen Schlüssels zu einer Entität. Dieses Problem kann durch die Verwendung von digitalen Zertifikaten im Rahmen einer PKI gelöst werden.

Tabelle 27 listet die im VPN-Umfeld verwendeten asymmetrischen Algorithmen auf.

Name	**Zugrunde liegendes math. Problem**	**Anmerkungen**	**VPN-Verwendung**
RSA (Rivest, Shamir, Adleman)	Faktorisierung großer Zahlen	Benannt nach Anfangsbuchstaben der Nachnamen der Algorithmuserfinder Ron Rivest, Adi Shamir und Len Adleman	IPSec, SSL
ElGamal	Diffie-Hellman-Problem (diskrete Logarithmen großer Zahlen)	Benannt nach dem Erfinder Taher ElGamal. Wird in manchen Quellen als Diffie-Hellman-Verschlüsselung bezeichnet.	
Digital Signature Algorithm (DSA)	Diffie-Hellman-Problem	Basiert auf ElGamal, wurde jedoch so entwickelt, dass es lediglich zur Signierung im Digital Signature Standard (DSS) verwendet werden kann, um den US-amerikanischen Exportbeschränkungen zu genügen.	IPSec, SSL
Elliptic Curve Cryptography (ECC)	Diskreter Logarithmus einer elliptischen Kurve über einen endlichen Körper	Bietet mit relativ kleinen Schlüssellängen eine starke Verschlüsselung	IPSec[1)]

Tabelle 27: Asymmetrische Algorithmen

Erläuterung zur Tabelle:

1) Lediglich als alternativer Teil des Schlüsselaustauschs verwendet.

Anlage 4.4 Hybride Verschlüsselung

Die asymmetrischen Verschlüsselungsalgorithmen sind wesentlich aufwändiger - und somit rechenintensiver - als die symmetrischen. Aus diesem Grund werden die erstgenannten in der Praxis nicht zur Verschlüsselung oder Signierung ganzer Nachrichten verwendet.

In der Regel verwendet man hybride Verfahren. Bei diesen Verfahren werden die Nachrichten mit einem zufällig ausgewählten symmetrischen Schlüssel verschlüsselt. Dieser wird anschließend mit dem öffentlichen Schlüssel verschlüsselt und so mit der verschlüsselten Nachricht versendet. Der Kommunikationspartner kann mit seinem privaten Schlüssel den symmetrischen Schlüssel entschlüsseln und mit dem Ergebnis dieser Entschlüsselung die eigentliche Nachricht entschlüsseln.