abc
nformation
IT Solution Company

NGN - Next Generation Network

NGN - Next Generation Network 1
1 Funktionelle Anforderung an das NGN 3
2 NGN Netzarchitektur 3
3 IPsec - Security Architecture for IP 4
3.1 IPsec Vertrauensstellungen - Security Association 5
3.2 Tunneling und Verschlüsselung 5
3.3 AH - Authentication Header 6
3.4 ESP - Encapsulating Security Payload 6
3.5 Ablauf zum Aufbau einer IPsec-VPN 7
3.6 VPN mit IPsec in der Praxis 7
4 VPN - Virtual Private Network 8
4.1 Tunneling 9
4.2 Tunneling-Protokolle 9
4.3 Systemanforderungen 9
5 L2TP - Layer-2-Tunneling-Protocol 10
5.1 L2TP-Architektur 10
5.2 L2TP über eine Firewall 11
6 PPTP - Point-to-Point Tunneling Protocol 12
6.1 PPTP-Architektur 12
6.2 PPTP über ein Firewall 12
7 Vernetzung von Telefonanlagen 13
7.1 Wählleitung über das öffentliche Telefonnetz 13
7.2 Analoge Festverbindung 13
7.3 Vernetzung über moderne Kommunikationswege 13

abc Information GmbH
PO Box 130208
13601 Berlin
Germany

+49-700-ITBROKER
http://www.Broker.de
email:contact@Broker.de

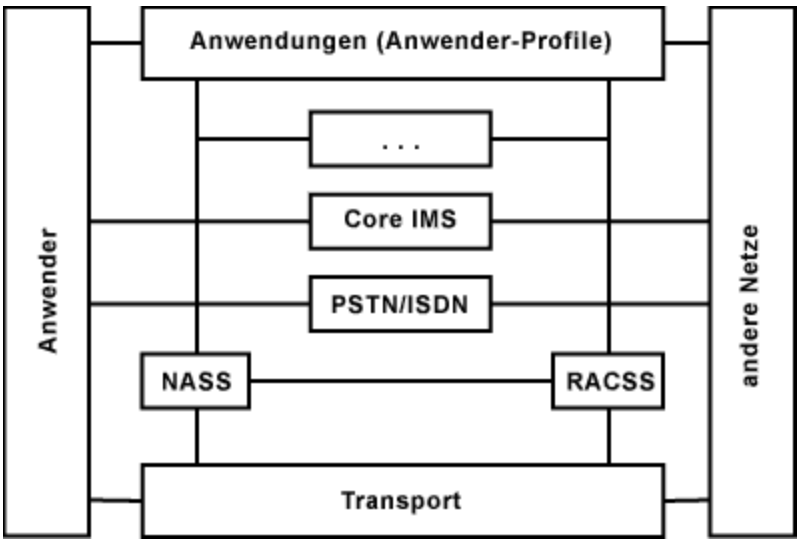
Die Liberalisierung des TK-Marktes führte zum Preisverfall bei der Festnetztelefonie. Telefonie und Breitband muss nicht mehr von einem Anbieter kommen. Alle Kommunikationsdiente, dazu gehört auch Telefonie, wandern auf eine Plattform, in ein Netz, das auf dem Internet-Protokoll (IP) basiert. Dazu ist ein neues Netz mit einer eigenen Netzarchitektur erforderlich. Dieses neue Netz nennt sich Next Generation Netzwork (NGN).

NGN ist ein Netz für alle Dienste und Anwendungen. Ein NGN muss flexibel sein, damit neue Dienste schnell und effizient eingeführt werden können. Bestehende Dienste müssen in die einheitliche Netzarchitektur integriert werden. Die wachsende Datenmengen müssen wirtschaftlich transportiert werden.
Kostenersparnis ist ein wesentlicher Teil des NGN. Durch die Beschränkung auf eine Systemtechnik kann man die Standorte und Flächen reduzieren. Es werden weniger verschiedene Ersatzteile gebraucht. Und es ist auch nur ein einziges Managementsystem notwendig, das betrieben und auf das die Mitarbieter geschult werden müssen.
Immer mehr Netzintelligenz zum Anwender hin. Bei ISDN gibt es den NTBA, der Teil des Netzes vom Netzbetreiber ist, aber beim Kunden installiert ist. Erst hinter dem NTBA gebinnt das Kommunikationsnetz des Kunden.
Ein NGN trennt zwischen dienstbezogenen Funktionen und den Transport-Funktionen. Das NGN stellt den Diensten Bandbreite und Dienstgüten zur Verfügung. Neben Punkt-zu-Punkt-Verbindungen sind auch Punkt-zu-Mehrpunkt-Verbindungen möglich. Viele Dienste sind heute schon IP-basiert. Deshalb bildet das Internet-Protokoll (IP) die Konvergenzschicht des NGN und interagiert mit der darunterliegenden Ethernetschicht. Ethernet-basierte IP/MPLS-Netze transportieren den wachsenden Datenverkehr kostengünstig und effizient. Ethernet-Komponenten sind weit verbreitet und günstiger als andere Vermittlungssysteme und Architekturen. Die bestehenden TDM-Netze werden schrittweise auf das neue NGN umgesetzt.

1 Funktionelle Anforderung an das NGN

- Benutzerauthentifizierung, -autorisierung und -abrechnung
- Konfigurationsmanagement auf Element-, Netz- und Dienstebene
- Leistungs- und Fehlermanagement
- Abwehr von Angriffen
- regulatorische und gesetzliche Maßnahmen

2 NGN Netzarchitektur



Das NGN teilt sich in eine Transport- und Anwendungsschicht. Die Transportschicht wird durch das Network-Attachment- Subsystem (NASS) und das Resource-Admission-Control-Subsystem (RACSS) gesteuert. Das NASS unterstützt die IP- Adressvergabe. IP-Schicht-Authentifizierung, Autorisierung und Zugangsnetzkonfiguration basieren auf Benutzerprofilen. Das RACSS ist die Zugangskontrolle die auf den Benutzerprofilen, den Betreiberregeln und den Transportnetzressourcen beruht.
Das Core IMS ist ein Dienst-Subsystem. Es ist eine Untermenge des IMS (IPMultimedia Subsystem), eine offene Systemarchitektur, die unabhängig von der Zugangstechnik IP-basierte Dienste unterstützt. Für die herkömmliche Telefonie (analog/ISDN) gibt es ein Emulationssubsystem.

3 IPsec - Security Architecture for IP

IPsec ist eine Erweiterung des Internet Protocols (IP) um lokale Netze zu einem gemeinsamen virtuellen Netz (VPN) über ein unsicheres Netzwerk (z. B. das Internet) miteinander zu verbinden. Zur Realisierung eines VPN gibt es neben IPsec auch L2TP (Layer 2 Tunneling Protocol) und PPTP (Point- to-Point Tunneling Protocol). IPsec wurde von der Internet Engineering Task Force(IETF) als integraler Bestandteil von IPv6 entwickelt. Dabei wurde aber sichergestellt, das die IPsec-Verfahren und Protokolle auch mit IPv4 nutzbar sind.
IPsec beinhaltet umfassende Sicherheitsfunktionen. Damit bietet IPsec alle Vorraussetzungen, die ein sicheres VPN ohne externe Protokolle benötigt.

- Interoperalitität
- kyptografischer Schutz der übertragenen Daten
- Zugangskontrolle
- Datenintegrität
- Authentifizierung des Absenders
- Verschlüsselung
- Authentifizierung von Schlüsseln
- Verwaltung von Schlüsseln

3.1 IPsec Vertrauensstellungen - Security Association

Hauptbestandteil von IPsec sind die Vertrauensstellungen (Security Association) zwischen zwei Kommunikationspartner. Diese müssen nicht zwangsläufig zwischen den Endpunkten (Client) einer Übertragungsstecke liegen. Es reicht aus, wenn z. B. bei der Kopplung zweier Netze die zwei Router über eine Vertrauensstellung verfügen. Selbstverständlich dürfen auch mehrere Vertrauensstellungen für eine Verbindung vorhanden sein.
Die Vertrauensstellungen regeln die Kommunikation von IPsec. Diese relativ flexiblen Kombinationen von Vertrauensstellungen erfordern einen sehr hohen Konfigurationsaufwand. Um eine gesicherte Verbindung zwischen zwei Stationen aufbauen zu können, müssen auf beiden Seiten viele Parameter ausgetauscht werden:

- Art der gesicherten Übertragung (Authentifizierung oder Verschlüsselung)
- Verschlüsselungsalgorithmus
- Schlüssel
- Dauer der Gültigkeit der Schlüssel.

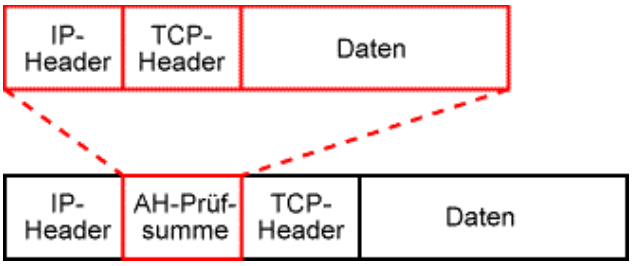
Vertrauensstellungen werden durch den Austausch vorab definierter Schlüssel hergestellt. Eine andere Form ist die Vergabe von Zertifikaten durch ein Trust-Center oder einen installierten Zertifikate-Server. Schlüssel und Zertifikate sollen sicherstellen, dass derjenige welcher einen Schlüssel oder ein Zertifikat besitzt, auch der ist, für den er sich ausgibt. Ähnlich wie bei einem Personalausweis, mit sich eine Person gegenüber einer anderen Person ausweist.
Schlüssel oder Zertifikat, ganz egal, beide Methoden benötigen viel Zeit und Sorgfalt bei der Einrichtung.
Die einfache Variante ist der geheime Schlüssel. Wichtig ist, dass die beiden Endpunkte über IP- Adresse, Subnetzmaske, Tunnelname und den geheimen Schlüssel bescheid wissen. Dazu gibt es weitere Parameter, die die Details der Authentifizierung und Verschlüsselung insbesondere die Länge des Schlüssels festlegen.

3.2 Tunneling und Verschlüsselung

Die zentralen Funktionen in der IPsec-Architektur sind das AH-Protokoll (Authentification Header), das ESP-Protokoll (Encapsulating Security Payload) und die Schlüsselverwaltung (Key Management).
Für den Aufbau eines VPN gibt es in IPsec den Authentication Header (AH) und den Encapsulating Security Payload (ESP). Beide können gemeinsam oder alleine genutzt werden. In beiden Verfahren findet eine gesicherte Übertragung statt.
Das AH-Protokoll sorgt für die Authentifizierung der zu übertragenen Daten und Protokollinformationen. Das ESP-Protokoll erhöht die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus. Zur Schlüsselverwaltung gibt es zwei Wege, um die Verwaltung und Verteilung der Schlüssel innerhalb eines VPN

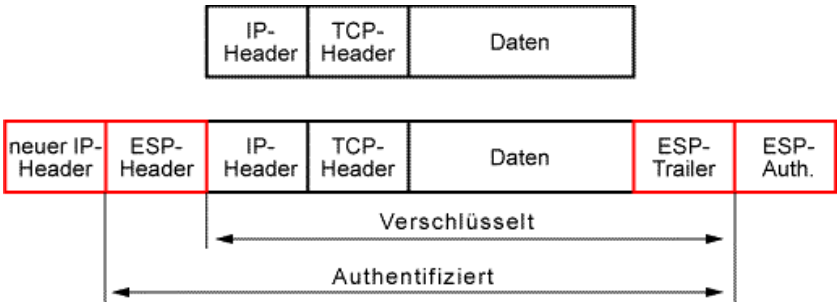
durchzuführen. Neben der reinen manuellen Schlüsselverwaltung, kann auch das Internet Key Exchange Protocol (IKE) eingesetzt werden.
IPsec setzt kein bestimmtes Verschlüsselungs- und Authentifizierungsverfahen voraus. Gängige Verfahren sind DES, Triple-DES (3DES) und SHA-1. IPsec-Implementierungen müssen kein bestimmtes Verfahren beherrschen. Die Zusammenarbeit unterschiedlicher VPN-Produkte muss deshalb vor ihrem Einsatz geklärt werden.
Die Firewall muss auf beiden Seiten die verschlüsselten Datenpakete durchlassen. Die Authentifizierung erfolgt über den UDP-Port 500, die verschlüsselten Datenpakete werden über das IP-Protokoll 50, dem ESP (Encapsulated Security Payload), verschickt. Dabei muss beachtet werden, dass Netware- Dienste über IPX nicht über die VPN-Verbindung funktionieren. Mit IPsec sind nur Dienste möglich, die auch IP verwenden.

3.3 AH - Authentication Header



AH bildet über das gesamte IP-Datenpaket eine Prüfsumme und fügt sie zwischen dem IP-Header und dem TCP-Header in das zu übertragende Paket ein. Über die Prüfsumme ist beim Empfänger die Vollständigkeit und Korrektheit der Daten und die Identität des Absenders feststellbar. Dieses Verfahren bereitet Probleme im Zusammenhang mit einem NAT-Router. Denn die Absender-Adresse stimmt mit der Adresse im Orginal-Header nicht überein. Der NAT-Router manipuliert die IP- Adressen. Dadurch wird ein solches Datenpaket beim Empfänger als ungültig verworfen.

3.4 ESP - Encapsulating Security Payload

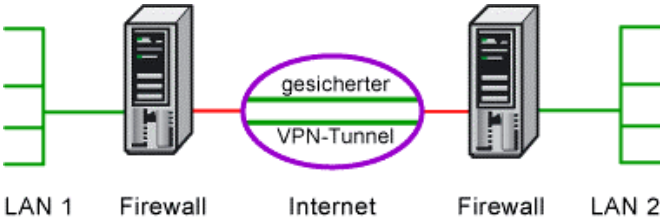


ESP beinhaltet zwei Betriebsmodi. Den Tunnel-Modus und den Transport-Modus. Der Tunnel-Modus wird eingesetzt, wenn zwei Netzwerke über eine unsichere Strecke miteinander verbunden werden sollen. Es wird dann das komplette IP-Datenpaket vor der Übertragung verschlüsselt. Davor wird dann ein neuer IP-Header gesetzt.
Im Transport-Modus werden lediglich die Daten verschlüsselt und der alte IP-Header unverändert belassen. Die Daten sind so zwar geschützt. Ein Angreifer kann jedoch zumindest eine bestehende VPN-Verbindung zwischen zwei Stationen feststellen.

3.5 Ablauf zum Aufbau einer IPsec-VPN

Das eine Ende von zwei VPN-Endpunkten generiert eine Anfrage an das Zielsystem. Das Zielsystem antwortet und leitet den Schlüsselaustausch per Internet Key Exchange (IKE) ein. Beide Endpunkte handeln dabei die zuverwendenden Verschlüsselungs- und Authentifizierungsverfahren aus. Über einen Schlüssel oder ein Zertifikat, das beide System kennen, wird eine Vertrauensstellung zueinander hergestellt. Für beide Seiten wird dann der digitale Master-Schlüssel erzeugt.
Beide Seiten legen dann die Verschlüsselungs- und Authentifizierungsverfahren für die Datenübertragung fest. Mit dem Master-Schlüssel wird der Schlüssel für die Datenübertragung erzeugt. Die Daten werden dann ausgetauscht und die Verbindung hergestellt.

3.6 VPN mit IPsec in der Praxis



Die Netzwerkteilnehmer im LAN 1 können auf das LAN2 zugreifen bzw. umgekehrt die Teilnehmer aus LAN 2 auf das LAN 1. Die Verbindung über das Internet läuft über einen verschlüsselten Tunnel ab.
Die beiden Firewalls müssen beim Verbindungsaufbau ihre Identität eindeutig nachweisen. Somit ist unberechtigter Zugang ausgeschlossen. Die Kommunikation über das Internet erfolgt verschlüsselt. Sollte ein Dritter die Datenpakete protokollieren erhält er nur Datenmüll.
Damit beide Firewalls miteinander kommunizieren können müssen die Adressen der jeweiligen anderen Station bekannt sein. Ändert sich die IP-Adresse eines Netzes, z. B. beim Verbindungsaufbau zum Provider, dann müssen die Adressen per dynamische DNS-Einträge ausgetauscht werden. Z. B. mit DynDNS.
Damit das Routing zwischen den Netzen funktioniert müssen die Adressbereiche unterschiedlich sein. Da die beiden Netze nach der Zusammenschaltung sich wie eines verhalten, dürfen IP-Adressen nicht doppelt vorkommen. Deshalb muss vorab auf beiden Seiten ein eigener Adressbereich, also unterschiedliche Subnetze konfiguriert werden.

4 VPN - Virtual Private Network

Netzwerke, die sich an zwei verschiedenen Orten befinden lassen sich über eine angemietete direkte Standleitung verbinden. Diese Standleitung entspricht in der Regel einer physikalischen Festverbindung zwischen den beiden Standorten. Die Unterhaltung dieser Festverbindung ist in der Regel sehr teuer, da der Netzbetreiber und seine Dienstleistung exklusiv bezahlt werden muss.
Da jedes Netzwerk in der Regel eine Verbindung zum Internet hat, bietet sich diese Verbindung zur Zusammenschaltung von zwei oder mehreren Netzwerken an (LAN-to-LAN-Kopplung).

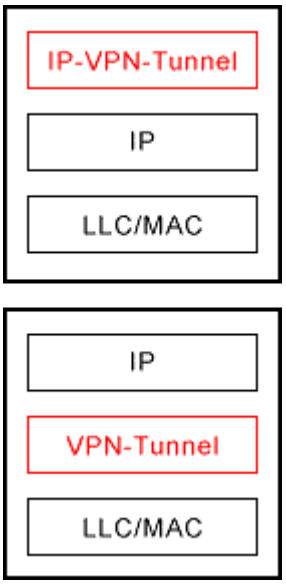
Das Internet hat den Nachteil, dass dessen Infrastruktur im Detail nicht bekannt ist und der Weg der Datenpakete zwischen LAN 1 und LAN 2 nicht nachvollziehbar oder vorhersagbar und kontrollierbar ist. So ist es an jedem Knoten, an dem ein Datenpaket überquert, möglich, dass es abgehört, verändert oder gelöscht wird. Die Daten werden also ungesichert über das Internet übertragen.

Um die Kosten einer Festverbindung zwischen LAN 1 und LAN 2 einzusparen und eine gesicherte Datenübertragung über das unsichere Internet zu gewährleisten, wird ein VPN, ein virtuelles privates Netzwerk, eingerichtet. Dazu wird mit einem Tunneling- Protokoll eine verschlüsselte Verbindung, der VPN-Tunnel, aufgebaut. Unabhängig von der Infrastruktur sorgen VPNs für eine angemessene Sicherheit der Daten, die darüber übertragen werden.
VPN-Lösungen ermöglichen zudem die kostengünstige und sichere Anbindung von ...

- Aussenstellen oder Niederlassungen(Filialen)
- kleine LANs
- Heimarbeitsplätze
- mobile Benutzer (Aussendienst)

Im Vordergrund steht dabei der geringe technische und finanzielle Aufwand für die sichere Anbindung in die unternehmensweite IT-Infrastruktur.

4.1 Tunneling



Für das Tunneling gibt es zwei Ansätze. Im einen Ansatz wrid auf der Schicht 3 des OSI-Schichtenmodells das Tunneling aufgebaut. Dabei wird zur Adressierung der Schicht bzw. des Datenpaketes das Internet Protocol (IP) verwendet. Man spricht dann vom IP-in-IP-Tunneling. In der Regel wird IPsec für diese Lösung verwendet.
Ein anderer Ansatz greift direkt auf der Schicht 2 des OSI-Schichtenmodells ein. Hier wird das Datenpaket der Schicht 3 verschlüsselt und dann mit der physikalsichen Adresse adressiert. In der Regel werden PPTP oder L2TP für diese Lösung verwendet.

4.2 Tunneling-Protokolle

- **PPTP (Point-to-Point Tunneling Protocol)**
  Das PPTP ist ein Punkt-zu-Punkt Tunneling Protokoll, das ursprünglich für RAS (Remote Access Server) entwickelt wurde. PPTP erlaubt die gegenseitige Authentifizierung beim Aufbau einer VPN-Verbindung.

- **L2TP (Layer 2 Tunneling Protocol)**
  L2TP ist eine Weiterentwicklung aus PPTP von Microsoft und L2F von Cisco. Es unterstützt verschiedene Protokolle und mehrere unabhängige, parallele Tunnel.

- **IPsec (IP Security)**
  IPsec ist im OSI-Schichtenmodell in der 3. Schicht angesiedelt und kann nur in IP-Netzwerken eingesetzt werden.

4.3 Systemanforderungen

Durch die Verschlüsselung der Daten innerhalb eines VPN entsteht ein zusätzlicher zeitlicher Aufwand, der ein längere Paketlaufzeit zur Folge hat. Bei der Planung eines VPN ist deshalb auf ein gute Ausstattung des gesamten Systems zu achten. Generell sollte man Hardware-Lösungen vorziehen. Sie arbeiten oftmals schneller und zuverlässiger als Software-Lösungen.
VPN im Zusammenhang mit einer Firewall führt häufig zu ungeahnten Problemen. Gerne wird für Firewall-Router der Pass-Through-Modus als VPN-Unterstützung angegeben. Vorzugsweise sollte man Router verwenden, die VPN direkt als Endpunkt unterstützen. Hier werden neben einzelnen VPN- Verbindungen auch Netz-Kopplungen möglich.

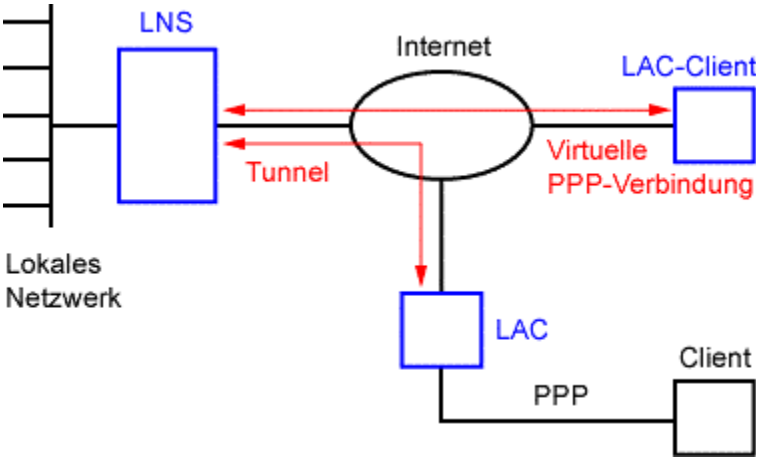
5 L2TP - Layer-2-Tunneling-Protocol

Das Layer-2-Tunneling-Protocol hat die Aufgabe PPP-Verbindungen über ein IP-Netzwerk zwischen zwei Netzwerk-Stationen oder zwei eigenständigen Netzwerken herzustellen. Ein Beispiel wäre ein Außendienstmitarbeiter, der mit seinem Notebook über eine Wählverbindung Zugang zum Internet hat und darüber eine getunnelte Verbindung zum Netzwerk seiner Firma unterhält, die über eine Standleitung ebenfalls ans Internet angebunden ist.
Anstatt einer reellen Punkt-zu-Punkt-Verbindung besteht die Übertragungsstrecke aus mehreren Routern, die miteinander verbunden sind. Für dieses Szenario gibt es zwei Protokolle:

- L2F - Layer-2-Forwarding
- PPTP - Point-to-Point Tunneling Protocol

Aus diesen beiden Protokollen entwickelte sich das Layer-2-Tunneling Protocol, wobei nahezu alle Anteile aus PPTP in L2TP eingeflossen sind. L2TP bietet jedoch den Vorteil, dass es jedes beliebige Netzwerkprotokoll in den PPP-Rahmen transportieren kann. PPTP unterstützt jedoch nur IP, IPX und NetBEUI.
L2TP bietet selbst keinen Authentifizierungs-, Integritäts- und Verschlüsselungsmechanismus. Der Schutz der getunnelten Daten muss z. B. mit IPsec erfolgen. In VPN-Lösungen kommt meist eine L2TP/IPsec-Lösung zum Einsatz.

5.1 L2TP-Architektur



Die L2TP-Architektur teilt sich in zwei logische Systeme: Den L2TP Access Concentrator (LAC) und den L2TP Network Server (LNS). Der LAC verwaltet die Verbindungen und stellt diese zum LNS her. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Das L2TP definiert die Kontroll- und Datenpakete zur Kommunikation zwischen dem LAC und dem LNS. Ein Network Access Server (NAS) stellt einen temporären Zugang für Remote-Systeme zu Verfügung. Der NAS kann im LAC oder im LNS implementiert sein.
Es gibt insgesamt zwei Szenarien einen L2TP-Tunnel aufzubauen. Das erste Szenario sieht eine PPP-Verbindung zwischen dem Client und dem LAC vor. Z. B. über das Wählnetz (analog oder ISDN). Der LAC tunnelt die PPP-Daten zum LNS und bekommt von diesem eine IP-Adresse aus dem LAN zugeteilt.
Das zweite Szenario sieht eine direkte Unterstützung von L2TP auf dem Client vor. Der Client ist dann selber der LAC. Die Daten werden genauso mit PPP übertragen. Die IP-Adresse aus dem LAN wird auch hier vom LNS zugeteilt. In beiden Fällen ist die Autorisierung und Authentifizierung von den Mechanismen im LAN abhängig. Das ist z. B. über den NAS möglich.

Mit L2TP wird ein Tunnel zwischen LAC und LNS aufgebaut. Der NAS identifiziert den Remote-User über einen Authentifizierungsserver. Ist die Authentifizierung erfolgreich wird der L2TP-Tunnel etabliert. Der LNS identifiziert sich ebenfalls beim Remote-User und bestätigt den L2TP-Tunnel. In diesem Tunnel wird für jede PPP-Verbindung eine Sitzung (Session) zwischen LAC und LNS aufgebaut. Mittels des Multiplex-Modus lassen sich in einem Tunnel mehrere Sitzungen aufbauen.
Innerhalb des PPP-Tunnels existieren zwei verschiedene Kanäle. In einem befinden sich die Kontrollnachrichten, in dem anderen die eigentlichen Nutzdaten. Der Kontrollkanal ist eine gesicherte Verbindung, der Datenkanal ist eine ungesicherte Verbindung. Die Nutzdaten werden also ungesichert in Klartext übertragen, sofern das Transport-Protokoll (PPP) keine Verschlüsselung unterstützt oder nicht aktiviert wurde.

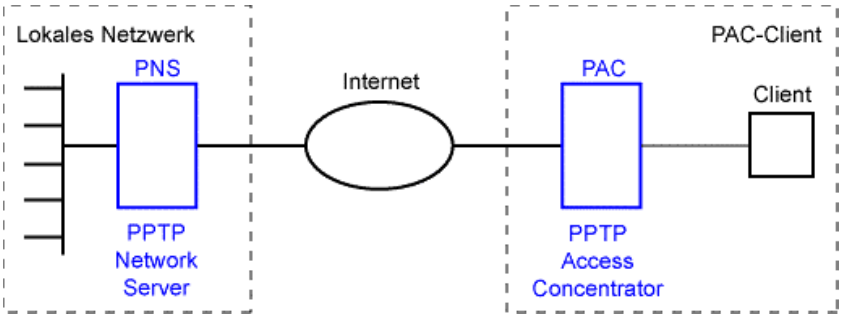
5.2 L2TP über eine Firewall

VPN über ein Firewall schließt sich meistens aus. Ohne Probleme ist VPN über eine Firewall nur möglich, wenn die Firewall gleichzeitig als Endpunkt einer VPN-Verbindung arbeitet.
Eine Firewall erwartet die Datenpakete von dem Port kommend, von dem sie zuvor angefordert wurden. L2TP arbeitet mitnichten so. L2TP antwortet in der Regel von irgendeinem freien Port über 1024. Um L2TP doch über eine Firewall zu nutzen, verwendet man eine Funktion mit dem Namen Port- Triggering. Damit wird auf einem bestimmten Port mit ausgehendem Datenverkehr das Freischalten weiterer Ports für eingehenden Datenverkehr ermöglicht. Bei L2TP währe der Triggering Port die 1701.
Dazu müssen die Ports 1025 bis 65535 freigeschaltet werden. Setzt die Firewall auf einen Portfilter wäre das eine riesige Lücke, was sie nahezu unbrauchbar macht.

6 PPTP - Point-to-Point Tunneling Protocol

Das PPTP wurde 1996 vom PPTP-Forum entwickelt. Es kommt hauptsächlich in Microsoft- Betriebssystemen zum Einsatz. Daher auch die häufige Nennung im Zusammenhang mit Microsoft.
PPTP ist ausschließlich für den Transfer von IP, IPX und NetBEUI über IP geeignet. Es baut auf den Remote Access Server für Microsoft Windows NT inklusive der Authentifizierung. Wegen der weiten Verbreitung von Windows 9x-Clients spielt PPTP beim Aufbau von VPNs in reinen Microsoft- Netzwerken eine große Rolle.

6.1 PPTP-Architektur



Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP Access Concentrator (PAC) und den PPTP Network Server (PNS). Der PAC verwaltet die Verbindungen und stellt diese zum PNS her. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.
Der PAC ist üblicherweise in den Client integriert und stellt eine PPP-Verbindung zum PNS her. Nach der Authentifizierung und Autorisierung wird dem PAC eine IP-Adresse aus dem LAN zugewiesen. Danach beginnt er PPTP-Pakete zu senden. Die PPP- Rahmen werden mit Generic Routing Encapsulation (GRC) verpackt. Danach werden die Datenpakete über das IP-Netz zum Ziel transportiert.
Eine Verschlüsselung findet nicht statt. Daher muss bereits bei PPP die Verschlüsselung ausgehandelt werden. Z. B. mit RC4, was Microsoft auch als Microsoft Point-to-Point-Encryption (MPPE) bezeichnet.

6.2 PPTP über ein Firewall

VPN über eine Firewall schließt sich meistens aus. Ohne Probleme ist VPN über eine Firewall nur möglich wenn die Firewall gleichzeitig als Endpunkt einer VPN-Verbindung arbeitet. Andernfalls ist es bei PPTP mit Port-Forwarding an das Zielsystem im lokalen Netz auch getan. Über den Port 1723 laufen alle Kontrolldaten einer PPTP-Verbindung. Dieser Port muss bei der Nutzung von PPTP von innen geöffnet sein, damit ein PPTP-Client die ausgehenden bzw. eingehenden Verbindungen nutzen kann.

7 Vernetzung von Telefonanlagen

Firmen und Organisationen streben generell eine Vereinfachung der Kommunikation unter ihren unterschiedlichen geografischen Standorten an. Dazu werden die Telefonanlagen an den verschiedenen Standorten miteinander verbunden. Man spricht dann von einer Vernetzung zu einem Corporate Network(CN) oder Private Network(PN).

7.1 Wählleitung über das öffentliche Telefonnetz

Die einfachste Form der Telefonanlagenvernetzung wird über eine Wählleitung des öffentlichen Telefonnetzes realisiert. Dazu verhält sich der Teilnehmer A bei der Herstellung der Verbindung zu Teilnehmer B, der sich in einer entfernten Telefonanlage befindet, wie bei der Verbindungsaufnahme in seinem lokalen System. Die Telefonanlage übernimmt die Anwahl über das öffentliche Telefonnetz. Am Standort B geht der Anruf wie ein normaler Anruf über das Telefonnetz ein. Die Nutzung der Leistungsmerkmale aus den lokalen Systemen sind standortübergreifend nicht möglich, da die Übertragung nur für die akustische Signalisierung und die folgende Sprachübertragung ausgelegt ist.

7.2 Analoge Festverbindung

Bei einem hohen Gesprächsaufkommen zwischen Standort A und B wird die Nutzung von Wählleitungen auf Dauer zu teuer. Stattdessen wird eine analoge Festverbindung zwischen den Standorten eingerichtet. Diese Art der Dauerverbindung ist kostengünstiger. Für die Teilnehmer ändert sich nichts.
Standortübergreifende Leistungsmerkmale sind nur bedingt möglich. Nutzt der Hersteller der Telefonanlagen ein Protokoll für die Vernetzung seiner Systeme ist es durchaus möglich.

7.3 Vernetzung über moderne Kommunikationswege

Ist die Zeit von ISDN zu Ende? Wird der Anwendungsbereich von ISDN von NGN´s und VDSL geschluckt?

Im Laufe der Zeit und deren technische Entwicklung in Technik und Telekommunikation beschränkte sich die Übertragung der Sprache nicht nur zwischen zwei Telefonen. Heute findet im Bereich der Telekommunikation die Übertragung von Sprache, Daten, Texten, Bild und Video zwischen Mensch und Maschine statt.

ISDN als öffentliches Telekommunikationsnetz, hat entscheidend dazu beigetragen, dass eine standortübergreifende Kommunikation ohne Kompromisse möglich geworden ist.

Zur Vernetzung von Telefonanlagen werden folgende Kommunikationswege genutzt:

- Festverbindung(analog/digital)
- Richtfunk(meist als Backup-Lösung)
- HDSL(z.B. S_2M)

Die Vernetzung von Telefonanlagen eines Herstellers stellt heute kein großes Problem dar. Auch Kleinstanlagen im Soho-Bereich beherrschen dieses Leistungsmerkmal.
Bei großen Anlagen ist es aus Kostengründen und der Wirtschaftlichkeit(Fusionen/Aufkäufe/Joint Ventures) notwendig die TK- Systeme zweier Systemlieferanten zusammenzuschalten. Der Kunde hat bei dieser homogenen Vernetzung bei Problemen mindestens zwei Ansprechpartner. Um den Wünschen des Kunden gerecht zu werden hat das Standardisierungsgremium ETSI über ein Protokoll abgestimmt, das ein leistungsstarkes und standardisiertes Signalisierungssystem darstellt. Q.SIG ist das harmonisierte Protokoll um TK-Systeme und -komponenten verschiedener Hersteller zu vernetzen.

Beispiel einer reelen Testkonfiguration (alt):