# FACHHOCHSCHULE WEDEL

SEMINARARBEIT

in der Fachrichtung

Wirtschaftsingenieurwesen

SoSe 2018

Seminar: Informatik

Thema:

# Das Projekt:VPN-Gate


| | |
|---|---|
| Eingereicht von: | Hamit, Günaltay (Matrikelnr. 102122) |
| | E-Mail: hamit.guenaltay@gmail.com |
| Erarbeitet: | 5.Semester |
| Abgegeben am: | 14.05.2018 |
| Betreuer: | Prof. Dr. Michael Anders |
| | Fachhochschule Wedel |
| | Feldstraße 143 |
| | 22880 Wedel |
| | Tel. (0 41 03) 8048 - 24 |

# Inhaltsverzeichnis

Inhaltsverzeichnis……..1

1 Einleitung…….4

2 Proxy-Server……..……4

2.1 Was ist ein Proxy-Server……..…..4

2.2 Proxy-Arten…….5

2.2.1 Forward-Proxy-Server……..5

2.2.2 Reverse-Proxy-Server……..5

2.2.3 Transparente-Proxies……5

2.2.4 Anonyme-Proxies……..6

3 VPN(Virtual Private Network)……..7

3.1 Was ist ein VPN ?……..7

3.2 Geschichte und Technologie…….8,9

3.3 Warum VPN´s…….10

3.4 VPN-Typen……10,11

3.5 Tunneling-Protokolle……12

3.5.1 Point-to-Point-Tunneling(PPTP)……13

3.5.2 Layer 2 Tunneling Protocol (L2TP)……..……14

3.5.3 IP Security Protocol (IPSec)……..15

3.6 VPN-Vorteile……..…..16

4 Das Projekt „VPN-Gate“……17

4.1 Wie funktioniert VPN-Gate……17

4.2 Probleme mit herkömmlichen VPN-Diensten…….17,18

4.3 Vorteile VPN-Gate……..…..18

5 Fazit.……19

6 Quellen und
Literaturverzeichnis……20

# 1.Einleitung

Im August 2016 veröffentlichte die Zeitschrift „ZDNET“ unter dem Titel „VPN-Lösungen für Unternehmen im Überblick“ einen Artikel, der sich eingehend mit der Problematik und der Auswahl des VPN´s für Unternehmen beschäftigt.
Der Artikel geht darauf ein, das es kaum noch herkömmliche VPN´s gibt, sondern die meisten VPN´s in verschiedenen Varianten zur Verfügung gestellt werden.
Das Projekt „VPN-Gate“, könnte eine gute Variante sein, welches in der folgenden Arbeit analysiert wird.
Aber zunächst schauen wir uns Proxy-Server und Allgemein VPN´s an, um einen guten Einblick in die Thematik zu bekommen.

# 2.Proxy-Server

## 2.1 Was ist ein Proxy-Server

Ein Proxy (von englisch proxy representative„Stellvertreter“, von lateinisch proximus „der Nächste“) ist eine Kommunikationsschnittstelle in einem Netzwerk.

Die Komponente dient als Vermittler zwischen einem Endgerät, wie zum Beispiel einem Computer, und einem anderen Server, von dem ein Anwender oder Client einen Service anfordert. Der Proxy-Server kann sich dabei auch auf der gleichen Maschine wie ein Firewall-Server befinden. Denkbar ist aber natürlich auch ein separater Server, der die Anfragen durch die Firewall leitet. Der Vorteil eines Proxy-Servers ist, dass sein Cache alle Anwender bedienen kann. Werden eine oder mehrere Internetseiten häufig aufgerufen, befinden sie sich mit hoher Wahrscheinlichkeit im Cache des Proxies. Somit wird die Antwortzeit verkürzt. Ein Proxy kann auch die Interaktionen loggen, womit sich die Fehlersuche erleichtern lässt. Für den Anwender ist der Proxy-Server in der Regel unsichtbar. Alle Anfragen an das Internet und die entsprechenden Antworten sehen so aus, als hätte man direkt mit dem Internet kommuniziert. Tatsächlich ist der Proxy aber natürlich nicht wirklich unsichtbar, da zum Beispiel die IP-Adressen in den Einstellungen des Browsers konfiguriert werden muss. Anwender können online auf Web-Proxy-Server zugreifen oder ihre Web-Browser so konfigurieren, dass sie dauerhaft einen Proxy-Server verwenden.

## 2.2 Proxy-Arten

### 2.2.1 Forward-Proxy-Server

So genannte Forward-Proxy-Server schicken die Anfragen eines Clients zu einem Web-Server. Nutzer greifen auf Forward-Proxies zu, indem sie direkt auf eine Web-Proxy-Adresse zugreifen oder ihre Interneteinstellungen konfigurieren. Forward-Proxies erlauben das Umgehen einer Firewall und erhöhen Privatsphäre und Sicherheit für einen Anwender.

### 2.2.2 Reverse-Proxy-Server

Reverse Proxies behandeln alle Ressourcenanfragen am Ziel-Server, ohne dass der anfragende hierzu weitere Aktionen durchführen müsste.
Verwendung:

-Es gewährt indirekten Zugriff, wenn eine Website direkte Verbindungen aus Sicherheitsgründen nicht erlaubt

-Es kann Zugriff zu einer Seite deaktivieren. Denkbar ist das, wenn ein Internetanbieter oder eine Regierung bestimmte Website blockieren möchte

### 2.2.3 Transparente-Proxies

Die Transparenten Proxies zentralisieren den Netzwerk-Traffic. Bei Firmennetzwerken ist ein Proxy-Server mit einem Gateway-Server verknüpft oder sogar ein Teil davon. Damit trennt man das interne Netzwerk von externen Netzwerken, normalerweise also dem Internet. Eine Firewall schützt das Netzwerk vor äußerlichen Bedrohungen und ermöglicht es, dass man Daten aus Gründen der Security scannen kann, bevor man diese an einen Client im Netzwerk ausliefert. Diese Proxies helfen beim Monitoring und der Administration des Netzwerk-Traffics, da die Computer in einem Unternehmensnetzwerk in der Regel sichere Geräte sind, sie keine Anonymität benötigen und normalerweise alltägliche Aufgaben erfüllen.

### 2.2.4 Anonyme Proxies

Anonyme Proxies verschleiern die IP-Adresse des Clients. Somit lässt sich möglicherweise auf Inhalte zugreifen, die normalerweise von einer Firewall blockiert sind.

Hoch-anonyme Proxy-Server verbergen sogar den Umstand, dass sie von einem Client genutzt werden und präsentieren eine öffentliche Nicht-Proxy-IP-Adresse. Sie verschleiern also nicht nur die IP-Adresse des Clients, der sie verwendet, sondern erlauben auch Zugriff auf Websites, die möglicherweise Proxy-Server blockieren. Beispiele von starken Anonymisier-Proxies sind I2P und TOR (The Onion Router).

# 3.VPN(Virtual Private Network)

## 3.1 Was ist ein VPN?

Ein VPN(Virtuelles privates Netzwerk) ist ein Netzwerk, das ein öffentliches Netzwerk benutzt, um private Daten zu transportieren.
Die Aussage ist zugegebenermaßen eine recht allgemeine gehaltene Definition, die aber aller Arten von VPN´s gerecht wird. In der heutigen Zeit wird ein VPN sehr oft nur auf die Benutzung des Internets als öffentliches Netzwerk reduziert, was aber so nicht stimmt. Wie sie im folgendem sehen werden, gibt es eine ganze Reihe anderer, teilweise schon recht alter VPN-Technologien, die überhaupt keine Gebrauch vom Internet machen.
Aber zurück zur Definition eines virtuellen privaten Netzwerks. Das Gegenstück zum VPN ist ein echtes privates Netzwerk, also ein Netzwerk, das exklusiv von einem Unternehmen oder einer Organisation betrieben wird. Das heißt, alles Übertragungseinrichtungen und alle Übertragungsmedien gehören diesem Unternehmen oder sind ihm zur exklusiven Nutzung überlassen. Beispiele sind die so genannten Mietleitungen oder Standardfestverbindungen, die einer Organisation zur ausschließlichen Nutzung vermietet werden. Mit geeignetem Equipment zur Daten-oder Sprachübertragung über diese Leitungen wird ein scheinbar privates Netzwerk betrieben. Scheinbar deshalb, weil die Verbindungen zwar ausschließlich vom Mieter benutzt werden, jedoch meist, zumindest in Europa, Teil einer öffentlichen Netzwerkinfrastruktur sind. Diese Infrastruktur bietet jedoch umfassende Möglichkeiten zum Anzapfen dieser Verbindungen und stellt somit in jedem Fall ein mögliches Sicherheitsrisiko dar, auch wenn die Betreiber solcher Netze natürlich keinen Missbrauch treiben dürfen und ein Abhören nur aufgrund einer richterlichen Anordnung durch bestimmte Personen zulässig ist.
Ein öffentliches Netzwerk hingegen ist eine Kommunikationsinfrastruktur, die von einem Dienstleistungsunternehmen betrieben wird, das die Benutzung des Netzes jedermann gegen ein entsprechendes Verbindungsentgelt ermöglicht. Ein Beispiel hierfür sind öffentliche Telefonnetze. Jeder kann gegen eine entsprechende Gebühr dieses Netz benutzen.
Ein VPN versucht, private und öffentliche Netze zu kombinieren, indem das öffentliche Netzwerk als Trägernetzwerk für die private Kommunikation benutzt wird.

## 3.2 Geschichte und Technologien

Virtuelle private Netzwerke gibt es schon seit einiger Zeit. Sie wurden aber nicht immer so genannt. In der Vergangenheit wurden vielfach andere Begriffe verwendet. Eine ganze Reihe, teilweise schon recht lange im Einsatz befindlicher Technologien eignet sich als Basistechnologie für VPN´s:

-ISDN
-Frame Relay
-ATM
-Das Internet

ISDN:

Eine schon etwas ältere VPN-Technologie sind zum Beispiel die so genannten geschlossenen Nummernkreise in einem digitalen Netzwerk wie dem ISDN (Integrated Service Digital Network) ein leitungsvermittelndes, digitales Multiservice-Netzwerk. Das Telekommunikationsunternehmen vergibt hierbei für die Anschlüsse eines Kunden eine Reihe von Telefonnummern, die nur untereinander kommunizieren können. Verbindungen zu oder von Nummern außerhalb dieses Nummernkreises sind nicht möglich. Aus Sicht des Unternehmens sieht dies wie ein privates, abgeschlossenes Telefonnetz aus. In Wirklichkeit wird aber das öffentliche Netzwerk des Telekommunikationsunternehmens benutzt, das die nötige Infrastruktur in Form von Leitungen und Vermittlungssystemen zur Verfügung stellt.

Frame Relay:

Eine andere, ebenfalls bereits länger verfügbare VPN-Variante sind Netzwerke, die auf dem Frame-Relay-Verfahren basieren. Frame Delay ist eine Übertragungstechnologie, die ursprünglich zum reinen Datentransport entwickelt wurde, aber auch zunehmend für gemischte Sprach- und Datenübertragung verwendet wird.
Frame Relay ist aus der Sicht des Anwenders ein verbindungsorientiertes Protokoll. Das heißt, es muss eine sogenannte virtuelle Verbindung zwischen zwei Datenübertragungseinrichtungen existieren. Diese kann entweder vom Provider fest konfiguriert und dauerhaft aktiviert werden oder erst bei anstehender Datenübertragung vom Kunden aktiviert und anschließend wieder deaktiviert werden.

ATM:

Neben Frame Relay hat sich auch ATM(Asynchronous Transfer Mode) als Basis für die Art von öffentlichen Netzwerken etabliert, die sich sehr gut zum Aufbau von VPN´s eignen.
In einem ATM-Netzwerk ist es möglich sehr schnell Daten zu übertragen, aber das ist gar nicht einmal das wichtigste Kriterium für seine Auswahl, sondern es geht um die damit möglichen abgestuften Dienstqualitäten und die gute Eignung zur Übertragung von isochronen Datenströmen wie Sprache oder Video. Im Gegensatz zum Frame Relay-Verfahren, mit dem Daten von mehreren tausend Byte in einem Frame übertragen werden können, wird bei ATM das Cell Switching benutzt. Es werden dabei sehr kleine Zelle übertragen, die eine feste Länge von 53 Byte haben.
Die Nutzungspakete werden vor der Übertragung in 48 Byte große Zellen aufgeteilt, mit einem Header versehen und in den 53 Byte großen ATM-Zellen synchron übertragen.

Das Internet:

In neuester Zeit  wird immer öfter von IP-VPN´s oder auch Internet VPN´s gesprochen.
Der fundamentale Unterschied zu virtuellen Privaten Netzwerken auf Basis von ISDN,Frame Relay oder ATM ist der, dass die Trägertechnologie nicht auf der Ebene 2 des OSI-Schichtmodells, sondern auf der Ebene 3, der Netzwerkschicht, liegt.Der große Vorteil liegt darin, dass es möglich ist, damit von physikalischen Infrastrukturen unabhängig zu werden. Das IP-VPN transportiert IP-Pakete zwischen zwei Endsystemen. Ob das IP-Paket während der Übertragung in ATM,Frame Relay eingekapselt wird, ist aus Sicht des VPN unerheblich. Ein Internet-VPN benutzt das Internet, das weltgrößte und immer noch stark wachsende IP-Netzwerk, als öffentliches Netzwerk.

## 3.3 Warum VPN´s?

Der Hauptgrund für den Einsatz virtueller privater Netzwerke besteht in deren niedrigen Betriebskosten. Dies gilt insbesondere für Internet-VPN´s; bei VPN´s auf Basis von ATM und Frame Relay sind die Einsparungen längst nicht so hoch. Nicht selten sind die Gesamtkosten eines Internet-VPN´s, also die Summe aus Investition und den Betriebskosten, schon für das erste halbe Jahr geringer als unter Verwendung von traditionellen Netzwerkkomponenten. Somit gibt der Kostenfaktor meist den Hauptausschlag zugunsten dieser Technologie.

## 3.4 VPN-Typen:

End to End-VPN:
Wickeln zwei oder mehrere Computer ihre komplette Datenkommunikation verschlüsselt ab. Jeder Computer muss über die öffentlichen Schlüssel aller potentiellen Kommunikationspartner verfügen. Zusätzlich muss jede an der verschlüsselten Kommunikation beteiligte Arbeitsstation mit entsprechender VPN-Software ausgestattet sein.Zugangskontrollmechanismen regeln den beschränkten Zugriff der unterschiedlichen Arbeitstationen.


Abb.1: End to End-VPN

Site to Site-VPN:
Wird als Erweiterung interner LAN'S angesehen. Hier tauschen zwei Firmenstandorte ihre Daten über das Internet aus. Am Aufbau eines Internet-VPN'S sind zwei VPN-Gateways/ Firewall-Systeme beteiligt. Nur auf dem Weg zwischen den beiden VPN-Gateways erfolgt eine Verschlüsselung der Daten. Der Weg durch das lokale Netz vom Gateway zum Endgerät bleibt unverschlüsselt. Dadurch benötigen die Endgeräte keine zusätzliche VPN-Clientsoftware. Aufgaben der Gateway sind also, empfangene IP-Pakete für den Transport

über das Internet zu verschlüsseln, in ein neues IP-Paket einzupacken und zum Partner Gateway zu schicken, das den beschriebenen Vorgang wieder rückgängig macht.


Abb. 2: Site to Site-VPN

End to Site-VPN:
End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Außendienst) in ein Unternehmensnetzwerk eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Die VPN-Technik stellt eine logische Verbindung, der VPN-Tunnel, zum entfernen lokalen Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installiert sein. Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das entfernte Netzwerk.


Abb. 3:End to Site-VPN

## 3.5 Tunneling-Protokolle:

Das Tunneling ist die Basis moderner VPN´s. Mit Hilfe dieser Technologie ist es möglich Pakete eines Netzwerkprotokolls in Pakete eines anderen Netzwerkprotokolls zu kapseln und über dieses Netzwerk zu übertragen. Auf diese Weise ist es möglich zum Beispiel IPX-Pakete durch ein IP-Netzwerk transportieren. Eine andere, speziell für IP-Netze Interessante Anwendung ist das Verstecken von privaten, nicht registrierten Netzwerk- und Postadressen, indem IP in IP getunnelt wird. Auf diese Weise ist es möglich seine privaten Netze über das Internet miteinander verbinden. Hierbei werden die IP-Pakete gekapselt mit privaten Adressen, in Pakete mit offiziell registrierten IP-Adressen und wird transportiert durch das Internet zur Gegenstelle, die die Originalen Pakete wieder auspackt. Es gibt eine ganze Reihe von Tunneling-Protokollen, von denen jedoch zwei

eine besondere Rolle spielen: das Layer 2 Tunneling Protocol (L2TP) und das IP Security Protocol (im Tunnelmodus)

### 3.5.1 Point-to-Point Tunneling (PPTP)

Point-to-Point Tunneling Protocol, ist eines der ersten Tunnelprotokolle die es gab. Es wurde von Microsoft und Ascend entwickelt und es ist eine Erweiterung der PPP, des Point-to-Point Protocol. Es ist nicht nur eines der ersten, sondern auch eines der am weitesten verbreiteten Tunneling Protokolle, aufgrund seiner weltweiten Integration in Windows. Dieses Protokoll ermöglicht die Übertragung von IP-Paketen. Zur Authentifizierung dient bei PPTP CHAP/PAP. PAP steht für „Password Authentication Protocol“ und CHAP für „Challenge Handshake Protocol“. Bei PAP werden Login und Passwort im Klartext an den Zugangsserver geschickt und mit den Daten in der Datenbank verglichen. Bei Übereinstimmung erfolgt der Aufbau der Verbindung, ansonsten wird der Verbindungsaufbau abgelehnt. Ein sehr großer Nachteil dieser Authentifizierungsmehtode ist, dass alle Daten im Klartext über die Leitung geschickt werden und keinerlei Verschlüsselung stattfindet. Der Vorteil liegt in der einfachen Implementierung. Bei einer Authentifizierung mittels CHAP wird in 3 Schritten vorgegangen. Phase 1 ist die Initialisierungsphase, hier wird eine Verbindung zum Zugangsserver hergestellt. Dieser sendet einen so genannten Challenge, dies ist ein Zufallsstring. Der Client erhält diesen und errechnet aus dem Zufallsstring und dem Passwort einen MD53-Hash-Wert, dieser wird zusammen mit einer User-ID an den Server zurückgeschickt. Der Server schaut in seiner User-Datenbank nach und bildet aus dem String, den er dem Client gesendet hat und dem Passwort aus der User-Datenbank ebenfalls einen MD53 Hash-Wert und vergleicht den errechneten mit dem zurückgelieferten. Stimmen diese beiden überein wird die Verbindung aufgebaut, anderenfalls wird der Aufbau abgelehnt. Leider bietet PPTP keinerlei Möglichkeit zur Authentifizierung des Tunnel, d.h es wird nicht geprüft, ob die Daten, von der Person stammen mit der eine Verbindung aufgebaut wird. Auch ist das Verschlüsselungsverfahren ein sehr schwaches Verfahren, da die Verschlüsselung mittels des RC4-Verfahren erfolgt. Hier werden die Daten mit einem 40-128 Bit langen Schlüssel verschlüsselt, der aus dem Passwort abgeleitet wird.

### 3.5.2 Layer 2 Tunneling Protocol (L2TP)

Das Layer 2 Tunneling Protocol wurde primär für den Einsatz im Provider-Enterprise-Modell entwickelt. Wie Sie in der nachfolgenden Abbildung sehen, beginnt dabei der L2TP-Tunnel im Remote Access Concentrator (RAC) des Service Providers und endet in einem Gateway beim Kunden. Die Funktionalität der Tunnelendpunkte ist rollenbasierend der Tunnel wird von einem LAC(L2TP Access Concentrator) aufgebaut, der im RAC des Providers implementiert ist. Das entgegengesetzte Ende des Tunnels bildet der LNS, der L2TP Network Server, der entweder auf Routern oder auf speziellen VPN-Gateways implementiert ist. Der RAC des Service Providers erkennt an bestimmten Kennzeichen eines eingehenden Rufs( angerufene Nummer, Benutzer-ID usw.), ob es sich um eine Verbindung in das Netzwerk des Providers handelt oder ob die Verbindung zu einem Endkunden getunnelt werden soll. Dieses Verhalten wird auch zwangsweises Tunneling (Compulsory Tunneling) genannt, da der Client nicht selbst entscheiden kann, ob ein Tunnel aufgebaut wird oder nicht.

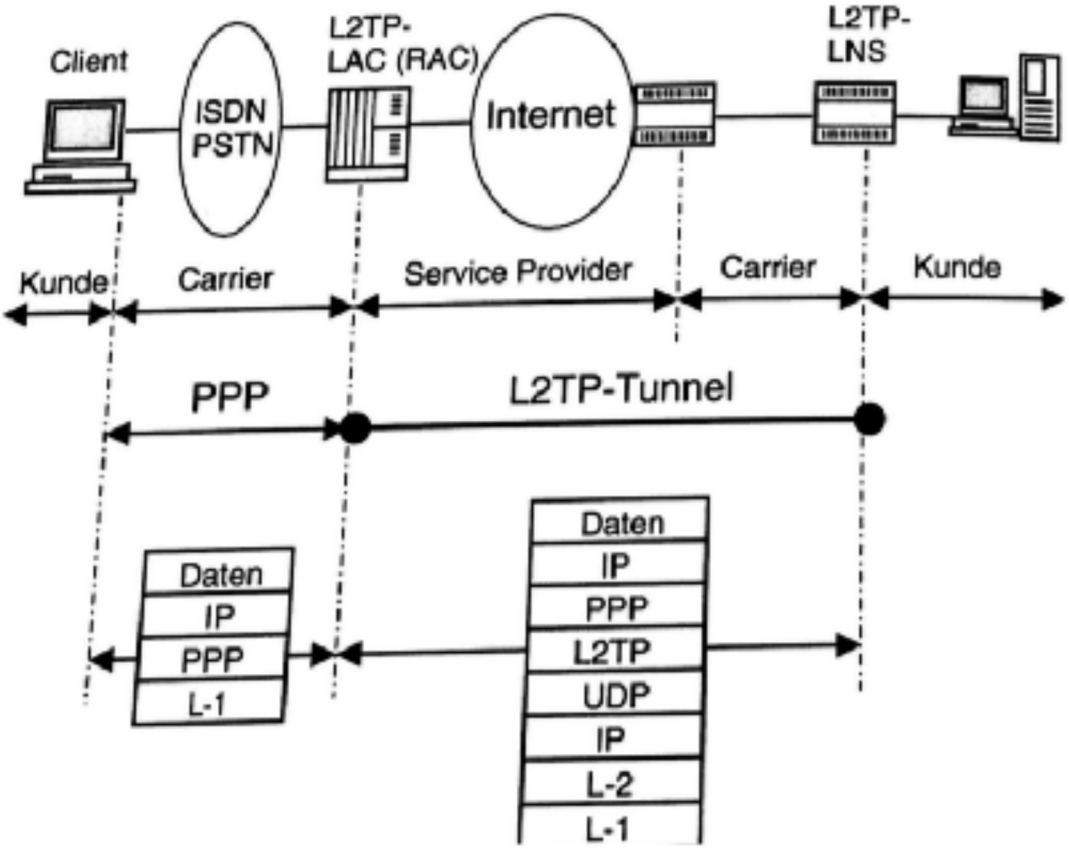


Abb. 4: L2TP-Modell

### 3.5.3 IP Security Protocol (IPSec)

IPSec im Tunnel-Modus dient meist als Basis für das Ende-zu-Ende-Modell.
Alle beteiligten Systeme müssen mit einer entsprechenden IPSec-Implementierung ausgerüstet sein. In der folgenden Abbildung sehen sie am Beispiel eines Remote-Access-VPN´s die Funktionsweise. Die IPSec-Tunnel beginnen und enden auf dem Endsystem des Kunden, meist einem Rechner mit IPSec-Clientsoftware und einem IPSec-Gateway. Die Carrier und Service Provider sind nicht am Tunneling und transportieren aus ihrer Sicht nur die IP-Pakete zwischen Client und Gateway. Das öffentliche Interface des IPSec-Gateways hat eine feste, offiziell registrierte IP-Adresse. Auch der Client bekommt bei der Einwahl in POP eines Service Providers eine offizielle IP-Adresse zugewiesen. Das private Interface des Gateway kann in einem nicht registrierten IP-Netzwerk liegen.

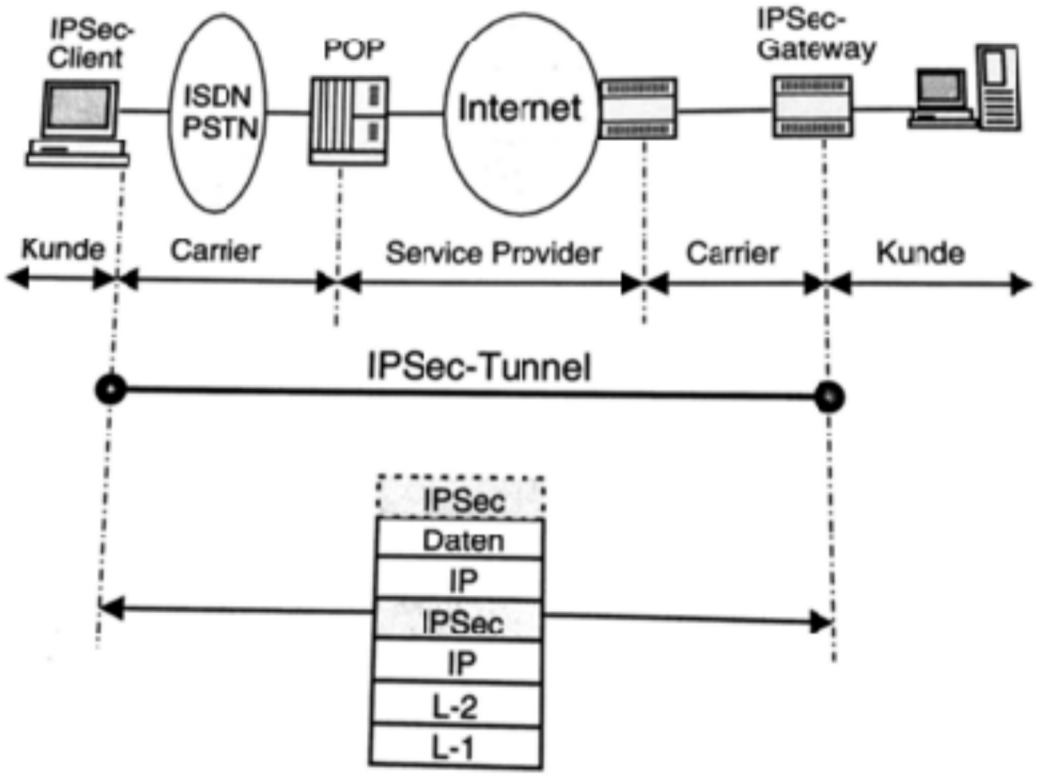


Abb. 5 : IPSec-Modell

## 3.6 VPN-Vorteile

-VPN kann die Firewall der Regierung umgehen.
Wenn die Firewall der Regierung nicht funktioniert oder wenn einige Websites im Ausland in der Firewall nicht erreichbar sind, ist es möglich darauf zu zugreifen, indem die Verbindung zu VPN-Servern außerhalb des aktuellen Aufenthaltsgebietes weitergeleitet wird.

-VPN kann die tatsächliche IP-Adresse verbergen
Während die Verbindung über einen VPN-Server weitergeleitet wird, ist die Quell-IP-Adresse, die dem Zielserver offengelegt wird, die des VPN-Servers, nicht die tatsächliche. Dies ist sehr hilfreich, da niemand auf die ursprüngliche IP-Adresse zurückfinden kann, wodurch das Risiko der Ausspähung ausgeschlossen wird.

-VPN kann Lauschangriffe verhindern
Bei der Verbindung von werden alle Übertragungen automatisch verschlüsselt. Selbst wenn das lokales Netzwerk von Snoopern kompromittiert wird, bleiben die Übertragungen intakt.

# 4.Das Projekt:“VPN-Gate“

VPN Gate Academic Experiment Project ist ein Online-Service als akademische Forschung an der Graduate School der Universität von Tsukuba, Japan. Der Zweck dieser Forschung ist es, das Wissen über "Global Distributed Public VPN Relay Server" zu erweitern.

## 4.1 Wie funktioniert VPN-Gate

VPN Gate-Netzwerk besteht aus vielen VPN-Servern, die von Freiwilligen auf der ganzen Welt zur Verfügung gestellt werden.
Windows, Mac, iPhone, iPad und Android werden unterstützt.
VPN-Gate unterstützt SSL-VPN (SoftEther VPN) -Protokoll, L2TP / IPsec-Protokoll, OpenVPN-Protokoll und Microsoft SSTP-Protokoll. Anonyme Verbindungen werden akzeptiert. Es sind keine Benutzerregistrierungen erforderlich. Jeder VPN-Server hat eine dynamische IP-Adresse. Daher kann es sich zu einer zufälligen Zeit ändern.
VPN-Server erscheinen und verschwinden zu jeder Zeit. Daher wird eine IP-Adresse möglicherweise nicht immer mit einem VPN-Server verbunden. Alle VPN-Server können den Datenverkehr ins Internet leiten, sodass die echte IP-Adresse verborgen bleibt.

## 4.2 Probleme mit herkömmlichen VPN-Diensten

Traditionelle VPN-Dienste werden von Unternehmen in ihren Rechenzentren gehostet. Diese traditionelle Art der Bereitstellung von gemeinsam genutzten VPN-Servern hat das Problem, dass sich die IP-Adressen der VPN-Server auf demselben oder einem ähnlichen IP-Adresszuweisungsblock befinden, im Allgemeinen weil die Server über denselben ISP gehostet werden. Außerdem sind diese IP-Adressen im Allgemeinen statisch, sodass sie sich selten ändern.
Ein solcher gemeinsamer VPN-Dienst ist schwach gegen "unbekannte Probleme an der Firewall der Regierung". Das "unbekannte Problem auf der Firewall der Regierung" weist normalerweise Probleme dahingehend auf, dass eine bestimmte IP-Adresse oder eine Reihe von IP-Adressen innerhalb des geschützten Bereichs vollständig unerreichbar sind. Wenn der "unbekannte Fehler" den IP-Adressbereich der IP-Adressblöcke ihrer VPN-

Server-Cluster trifft, werden alle VPN-Server innerhalb des Bereichs deaktiviert. In der Tat wird kürzlich berichtet, dass eines Tages ein bestimmter Cluster von traditionellen geteilten VPN-Servern plötzlich aus einem bestimmten Land unerreichbar wurde, in dem eine Firewall der Regierung läuft.
Ein weiteres Problem bei den herkömmlichen gemeinsam genutzten VPN-Servern ist die Verbindung der Bandbreite. Traditionelle gemeinsam genutzte VPN-Server sind physisch in einem Datencenter zusammengefasst. Alle von ihren Benutzern vorgenommenen Übertragungen werden auf eine bestimmte Zeile des Uplinks des Rechenzentrums konzentriert. Darüber hinaus wirken sich alle Arbeitsauslastungen auf die physischen Server aus, die die VPN-Server hosten. Der Dienstanbieter kann erwägen, die Servercluster zu erweitern oder den Uplink zu erzwingen, solche Erweiterungen sind jedoch kostspielig. Die Gebühr kann sich erhöhen, wenn solche Erweiterungen vorgenommen werden, oder andernfalls kann die Geschwindigkeit aufgrund der Kostenreduzierung fallen.

## 4.3 Vorteile VPN Gate

Es werden viele öffentliche VPN-Relay-Server von VPN Gate ausgeführt. Diese VPN-Server sind weder physisch in einem bestimmten Datencenter noch in einem bestimmten IP-Adressbereich platziert. Sie werden auf verschiedenen ISPs und an einer Vielzahl physischer Standorte gehostet.
Alle VPN-VPN-Relay-Server werden von vielen Freiwilligen verteilt und gehostet. Ein Freiwilliger ist eine Person, die einen Computer besitzt, der an das Breitband angeschlossen ist, das mit dem Internet verbunden ist. Ein Freiwilliger ist damit einverstanden, die CPU-Zeit und die Bandbreite bereitzustellen, um das VPN Gate Academic Experiment zu unterstützen. Freiwillige sind auf der ganzen Welt verteilt.
Die ISPs der Freiwilligen variieren ebenfalls. Daher sind die IP-Adressen jedes VPN-Servers verteilt und zeigen keine bestimmten Muster ihrer zugewiesenen IP-Adressen. Die Gesamtzahl der Freiwilligen ändert sich von Zeit zu Zeit, so wie die IP-Adressen der Server. Wenn also der Firewall der Regierung etwas zustoßen sollte, sollten die meisten VPN Gate Server diesen Vorfall überleben.
VPN Gate ist kostenlos verfügbar, da die Server von freiwilligen Helfern gehostet werden und sie nicht viel für die Bandbreite und CPU-Zeit ihrer Server ausgeben.

# 5.Fazit

Im ersten Teil der Arbeit haben wir uns Proxy-Server angeschaut, der als Zwischenspeicher fungiert. Er beantwortet Internet Anfragen deutlich schneller und verspricht eine gewisse Anonymität, da er seine eigene IP-Adresse an den Zielserver sendet. Jedoch gilt das nur für den http-Traffic, da sonst der Flash-Plug-In aus dem Browser auf den Zielserver greift, wodurch die tatsächliche IP-Adresse gesendet wird.
Im Zweiten Teil der Arbeit haben wir uns Allgemein VPN´s angeschaut , die eine gute Alternative zu teuren Standleitungen sind, da sie das Internet benutzen.
Im Hauptteil der Arbeit haben wir das Projekt „VPN-Gate“ kennen gelernt ,das durch freiwillig gehostete Server eine große Bandbreite an VPN-Server aus der ganzen Welt anbietet. Der Vorteil vom VPN-Gate zu herkömmlichen VPN-Diensten ist, dass es zum einen kostenlos ist und es keine Benutzerregistrierung benötigt, wodurch der Nutzer unkompliziert ein VPN-Server nutzen kann. Die Nachteile vom VPN-Gate sind, dass jeder Server einen anderen Hoster besitzt, wodurch nicht sicher gestellt werden kann, was die Person mit den Daten unserer eigenen IP-Adresse anstellt. Ebenfalls stellen Hoster nach einiger Zeit den Server nicht mehr zur Verfügung, wodurch der Nutzer fast jedes mal einen neuen Server aussuchen muss.

# 6. Quellen und Literaturverzeichnis

Manfred, Lipp (2002),VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit

D. Bachfeld: Sicheres Netz im Netz

http://www.vpngate.net/en/

https://en.wikipedia.org/wiki/Proxy_server

https://de.wikipedia.org/wiki/Virtual_Private_Network

https://www.zdnet.de/88275224/vpn-loesungen-fuer-unternehmen-im-ueberblick/

https://www.elektronik-kompendium.de/sites/net/0906191.htm

Abbildungsverzeichnis:

Abb.1: End to End-VPN : https://www.elektronik-kompendium.de/sites/net/0512041.htm

Abb. 2: Site to Site-VPN : https://www.elektronik-kompendium.de/sites/net/0512041.htm

Abb. 3:End to Site-VPN : https://www.elektronik-kompendium.de/sites/net/0512041.htm

Abb. 4: L2TP-Modell : Manfred, Lipp (2002),VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit

Abb. 5 : IPSec-Modell : Manfred, Lipp (2002),VPN - Virtuelle Private Netzwerke: Aufbau und Sicherheit