Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

Seminararbeit
Proseminar Rechnernetze

NAT & VPN
Adressübersetzung und Tunneling

Bastian Goerstner

28. Januar 2008

Betreut durch Arne Vater und Prof. Dr. Christian Schindelhauer

Abstract

NAT und VPN sind durch die Verbreitung von DSL fast in jedem privat Haushalt in Gebrauch. Für Unternehmen spielt VPN aufgrund von Globalisierung und der Möglichkeit, sich von überall ins Unternehmensnetz einwählen zu können, eine wichtige Rolle um Konkurenzfähig agieren zu können. NAT bietet die Möglichkeit, bis zur endgültigen Etablierung eines neuen Standards (z.B. IPv6) der durch IPv4 verursachten Adressknappheit entgegen zu wirken. Aus diesem Grund möchte ich auf die Funktionsweise und die Optionen, die diese Techniken bieten, in den nächsten Kapiteln genauer eingehen.

Inhaltsverzeichnis

1 NAT

1.1 Was ist NAT und wo kommt es zur Anwendung

NAT bedeutet "Network Address Translation "und kommt typischerweise in Firewalls, Switchen und Routern zum Einsatz. Es bedeutet ganz allgemein die transparente und automatisierte Abbildung, von Adressinformationen in Datenpaketen auf andere Adressen oder Ports. Dabei unterscheidet man zwischen 2 verschiedenen Arten: bei der klassischen Form handelt es sich um das sogenannte "Outbount NAT ", bei dem eine Verbindung nur in eine Richtung erfolgt und auf der anderen Seite um das "Two Way NAT "bei dem, wie der Name schon sagt, eine bi-directionale Verbindung möglich ist. Beim Outbound NAT gewann das Network Address Port Translation Protokoll, welches eine Umsetzung von IP-Adressen und Portnummern ermöglicht, in den letzten Jahren, immer mehr an Bedeutung. Mit dieser Technik wird versucht, der Knappheit der IPv4 Addressen entgegen zu wirken, dabei werden Addressen aus einem privaten IP- oder Portbereich auf eine gemeinsame öffentliche IP abgebildet. Dieses sogenannte Masquerading findet in jedem Home- bzw. Office Netzwerk statt.

1.2 Funktionsweise

Bei der Funktionsweise müssen 2 verschiedene Varianten betrachtet werden:

1. **Source NAT**

   Die private Quell-IP wird bei ausgehenden Paketen durch eine öffentliche noch freie IP ersetzt. Dieses Mapping von privater Quell-IP auf öffentliche Quell-IP wird abgespeichert.

local

Quell-IP	Ziel-IP
192. 168.1.1	84.56.214.162
192. 168.1.2	84.56.214.162
192. 168.1.3	84.56.214.162
192. 168.1.4	84.56.214.162

öffentlich

Quell-IP	Ziel-IP
64.233.183.99	84.56.214.162
66.205.71.102	84.56.214.162
132.230.167.230	84.56.214.162
195.71.11.67	84.56.214.162

Abbildung 1: Source NAT

2. **Destination NAT**

   Hierbei erfolgt der umgekehrte Prozess, bei dem das gespeicherte Mapping verwendet wird. Diese Speicherung ermöglicht es, für ein eingehendes Paket festzustellen durch welchen internen Client es angefordert wurde.

local

Quell-IP	Ziel-IP
84.56.214.162	192. 168.1.1
84.56.214.162	192. 168.1.2
84.56.214.162	192. 168.1.3
84.56.214.162	192. 168.1.4

öffentlich

Quell-IP	Ziel-IP
84.56.214.162	64.233.183.99
84.56.214.162	66.205.71.102
84.56.214.162	132.230.167.230
84.56.214.162	195.71.11.67

Abbildung 2: Destination NAT

1.3 Kategorisierung nach rfc 3489

Bei der Kategorisierung möchte ich auf den von der Network Working Group vorgestellten, STUN Standard (rfc 3489), zurückgreifen. Ich habe dieses Memo gewählt, da die von Ihr beschriebene Klassifizierung auch außerhalb dieses Standards verbreitet ist.

1.3.1 Full Cone

Alle Anfragen bei gleicher interner IP und Port werden mit derselben externen IP verknüpft. Dies ermöglicht aber jeden beliebigen externen Host mit einem internen Client in Verbindung zu treten, sobald er an die externe IP sendet. Wie leicht vorstellbar, birgt diese Variante starke Sicherheitsrisiken.

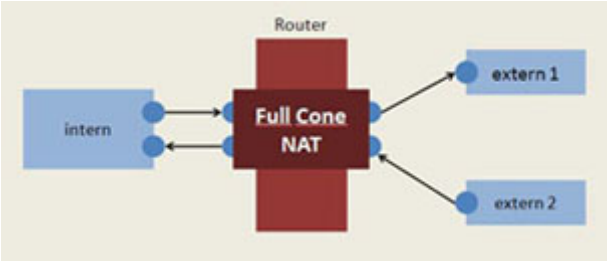

Abbildung 3: Full Cone NAT

1.3.2 Restricted Cone

Wie in Abbildung 4 verdeutlicht, wird das Full Cone NAT so eingeschränkt, dass nur ein externer Host mit IP Addresse X, an einen internen Daten senden kann, wenn dieser interne Client vorher eine Verbindung zu IP X aufgebaut hat.

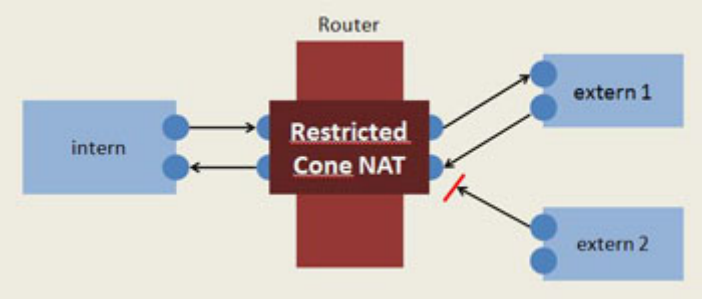

Abbildung 4: Restricted Cone NAT

1.3.3 Port Restricted Cone

Verschärft die Beschränkungen des Restricted Cone NAT weiter, indem nur der externe Host mit IP X und Port P Daten senden kann, wenn vorher genau an diesen Host X an Port P Daten gesendet wurden. Diese Situation wird in folgender Abb. noch einmal genauer verdeutlicht:

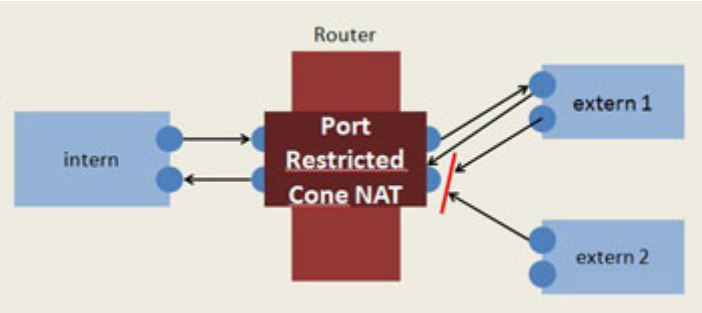

Abbildung 5: Port Restricted Cone NAT

1.3.4 Symmetric NAT

Bei dieser Variante erhalten eine interne IP und Port, die an einen bestimmten externen Host senden, die selbe externe IP. Baut dieselbe interne IP eine Verbindung zu einen anderen externen Host auf, erhällt sie auch eine andere externe IP. Wie in Abb. 6 zu sehen, ist auf diesen Weg, nur sehr schwer eine Verbindungsaufnahme möglich von außen nach innen möglich. Es kann nur der externe Port ein Paket senden, der vorher auch ein Paket erhalten hat.

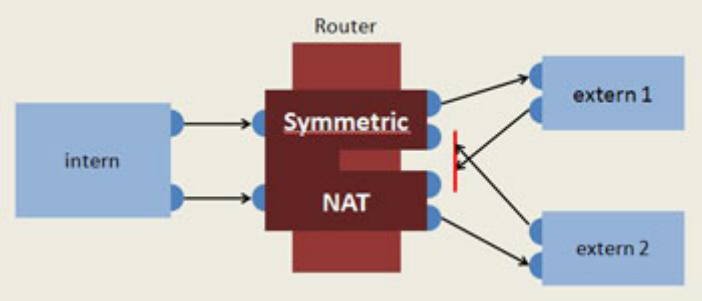

Abbildung 6: Symmetric NAT

Durch dieses Verfahren können zwar die Sicherheitsrisiken deutlich verkleinert werden, jedoch wird auf diese Weise ein externer Verbindungsaufbau fast unmöglich. NAT hat zudem den großen Nachteil, dass eine direkte End-to-End Kommunikation von Hosts, die durch NAT getrennt, sind kaum möglich ist. Daher ist eine Verwendung von z.B. Internet-Andwendungen, die eine von außen initierte Verbindung per TCP oder UDP

erfordern, nur schwer möglich. Große Vorteile bietet NAT aber bei der Bekämpfung von Angriffen von außen, da der Schutzmechanismus sich auf eine bestimmte Stelle im Netzwerk (Router) konzentriert werden kann.

2 VPN

2.1 Begriffsklärung und Anforderungen

VPN heißt "Virtual Private Network "und bedeutet, das ein öffentliches Netzwerk (z.B. das Internet) verwendet wird, um private Daten zu transportieren.

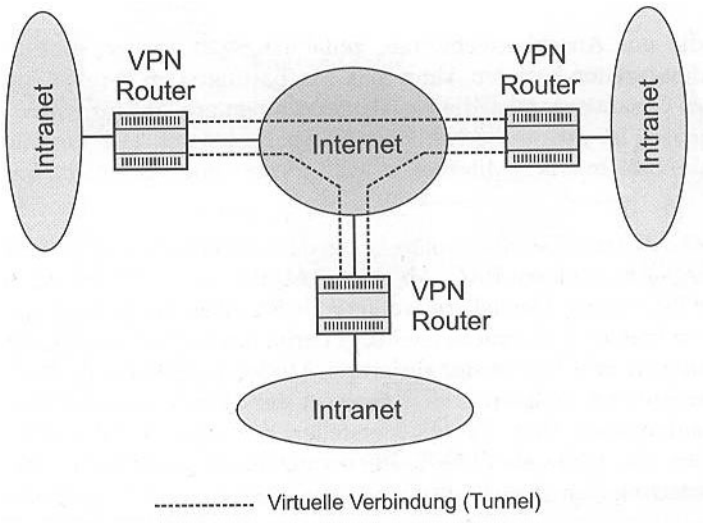

Abbildung 7: Manfred Lipp: VPN am Beispiel eines Brach Office VPN's in VPN Aufbau und Sicherheit, Seite 45

Um Missverständnisse zuvermeiden, möchte ich zuerst darauf eingehen, was überhaupt ein privates bzw. ein öffentliches Netzwerk ist. Von einem privaten Netzwerk spricht man, wenn das gesamte Netzwerk, insbesondere alle Übertragungsvorichtungen, von einem Unternehmen betrieben werden. Ein öffentliches Netzwerk dagegen ist eine Kommunikationsinfastruktur, die von einen Provider (Dienstleistungsunternehmen) betrieben wird und Jedem für eine entsprechende Vergütung zur Verfügung gestellt wird. VPN kombiniert diese 2 Netzvarianten, indem ein sogenannter Tunnel durch das öffentliche Netz aufge-

baut wird, um Daten zwischen 2 voneinander getrennten privaten Netzwerken auszutauschen. VPN-Netzwerke erlangen durch Globalisierung und Dezentralisierung zunehmend an Bedeutung, da z.B. ein Angestellter von zu Hause aus auf den Firmenserver zugreifen kann, oder es zwei Unternehmensstandorten auf diese Art ermöglicht wird, ein gemeinsames Netzwerk zuverwenden. Es ermöglicht für Unternehmen, Universitäten aber auch Privatpersonen eine größere Flexibilität, da über jedes beliebige bestehende öffentliche Netzwerk eine gesicherte Verbindung ins eigene Netz aufgebaut werden kann. Für Unternehmen stellt es zudem eine deutlich kostengünstigere Alternative zu den herkömmlichen SDSL / ADSL Leitungen dar, um Standorte miteinander zu verbinden.

Aus diesen vielseitigen Nutzungsmöglichkeiten lassen sich die enormen Anforderungen ableiten, die an ein VPN gestellt werden, die Manfred Lip, in seinem Buch über VPN, sehr gut zusammengefasst hat:

- *Sicherheit* (Datenvertraulichkeit, Schlüsselmanagement, Paketauthentifizierung, Datenintegrität, Benutzerauthentifizierung, Benutzerautorisierung, Schutz vor Sabotage, Schutz vor unerlaubten Eindringen
- *Verfügbarkeit*(Darf nicht schlechter sein wie in traditionellen WAN-Netzen)
- *Koexitenz zu traditionellen WAN Netzen*
- *Quality of Service*(Hohe Qualität muss auch in einem konvergenten Netz für Sprache, Daten und Videostreaming gewährleistet werden)
- *Skalierbarkeit und Miggrationsfähigkeit* (Think big - Start Small)
- *Integration in bestehende Netzwerke*(VPN muss sich leicht in ein schon bestehendes LAN integrieren lassen)
- *Interoperabilität* (Selbst unterschiedlichste Hardware zusammen in einem VPN zunutzen)
- *Addressmanagement*

Meiner Meinung nach kommt dem Punkt Sicherheit aber die größte Bedeutung zu und ich werde daher im folgendem vorwiegend auf diesen Punkt eingehen. Zuvor möchte ich aber einen Überblick über die 3 wichtigsten VPN Varianten geben.

1. *Remote Access VPN - Site to End* Das Remote Access VPN ermöglicht, von einem entfernten Standort den Zugriff auf ein Firmennetzwerk. Hierzu wird lediglich auf Unternehmensseite ein VPN-Gateway oder VPN-Router benötigt der die Verbindungen terminiert. Die Clients können sich über jedes beliebiege Übertragungsmedium (Modem, ISDN, DSL, UMTS, WLAN) und jeden beliebigen Internet Service Provider in das Unternehmensnetz einwählen. Auf diese Weise kann zum Beispiel

ein Angestellter von zu Hause, oder Unterwegs (Hotel) eine Verbindung herstellen, und somit von jedem beliebigen Standort seine Aufgaben erledigen.

2. *Branch Office VPN - Site to Site* Ein Branch Office VPN ersetzt die herkömmlichen WAN Verbindungen zwischen Unternehmensstandorten. Dazu wird in jeden Standort ein VPN Gateway/Router installiert, zwischen diesen dann ein VPN Tunnel aufgebaut wird. Dadurch ist es Unternehmen möglich, die oft enormen Kosten für WAN Anbindungen drastisch zu veringern und damit auch unabhängiger von einem speziellen Provider zu werden.
3. *Extranet-VPN* Ein Extranet-VPN ähnelt den bereits vorgestellten Typen, hat aber eine wichtige zusätzliche Eigenschaft. Im Gegensatz zu den anderen Arten die nur einen reinen privaten Zugang ermöglichen, bietet das Extranet-VPN die Möglichkeit einen limitierten und kontrollierten Zugang auch externen Personen zur Verfügung zustellen. Der normale interne Traffic erfolgt wie in den zuvor vorgestellten Varianten über den VPN-Router, der Zugang der Fremdfirma wird zusätzlich über die Firewall geregelt. So ist es z.B. möglich, Kunden einen limitierten Zugriff, auf bestimmte Bereiche des Unternehmensnetz, zu erlauben.

2.2 Tunneling Modelle

Es wird hauptsälich zwischen 3 verschiedenen standardisierten Tunneling Modellen unterschieden, die sich im Start bzw. Endpunkt des Tunnels unterscheiden. Abb. 8 verdeutlicht Start- und Endpunkt des Intra-Provider, Provider-Enterprise, sowie End-to-End Modells. Die Tunneling Protokolle sind nach der Schicht des ISO/OSI Modells benannt auf der das sogenannte “Tunneling”stattfindet.

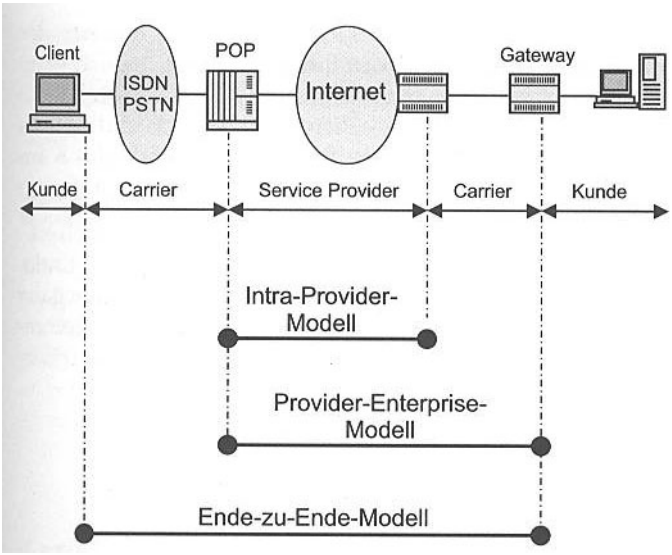

Abbildung 8: Manfred Lipp: Die drei grundsätzlichen Tunneling-Modelle in VPN Aufbau und Sicherheit, Seite 77

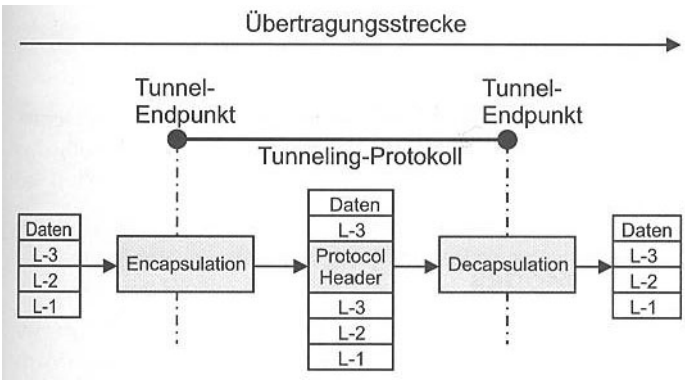

Abbildung 9: Manfred Lipp: Das Prinzip aller Tunneling-Protokolle in VPN Aufbau und Sicherheit, Seite 75

In Abbildung 9 werden in der Enkapselung die Pakete in andere Netzwerkpakete mit neuen Layer 3 Header eingefügt und anschließend ein Tunnel Header angehangen. An diesem angefügten Header erkennt der Empfänger, ob das Paket zu dem betreffenden

Tunneling Protokoll gehört und für ihn bestimmt ist. Dieser Header muss sich zwischen dem Layer-3 Header und den Nutzdaten befinden. Der Empfänger wertet schließlich den Header aus und entpackt die Daten. Diesen Prozess nennt man Dekapselung.

2.2.1 L2TP

Das Layer-2 Tunnel Protokoll wurde vornehmlich für den Einsatz als Provider-Enterprise Modell entwickelt. Dabei werden Pakete der Sicherungsschicht (Layer 2) in anderen Layer-2 Paketen verkapselt (z.B. mit Hilfe von Point-to-Point Rahmen in IP Paketen). Der Tunnel wird dabei vom L2TP Access Concentrator aufgebaut, der im Remote Access Connector (RAC) des Providers integriert ist. Der RAC erkennt ob es sich um normalen Datenverkehr (z.B. ins Internet) des Clients handelt oder ob ein Tunnel zu einen anderen Client erzeugt werden soll. Diese Erkennung kann z.B. mit Hilfe der Rufnummer oder der BenutzerID erfolgen. In L2TP sind aber keine Sicherheitsverfahren implementiert. Aus diesem Grund wird es immer häufiger in Verbindung mit IPSEC verwendet, worauf ich im nächsten Abschnitt noch genauer eingehen werde.

2.2.2 L3TP

Diese Tunneling Protokolle arbeiten auf der Netzwerkschicht, also eine Schicht höher wie die eben vorgestellten Tunneling Varianten. Sie haben aber im Gegensatz zu L2TP-Protokollen den großen Nachteil, das vermerkt werden muss, welche Art von Protokoll getunnelt wird, z.B. beim Einsatz von IPSec im Tunnelmodus wird ein IPSec-Header eingefügt. Dieses Verfahren kommt meist als End-to-End Protokoll zum Einsatz. Der IPSec-Tunnel beginnt in diesem Fall direkt beim Client. Der Endpunkt befindet sich in diesem Fall meistens auf einen IPSec Gateway des Clients. Bei dieser Variante ist der Service Provider nicht am Tunneling beteiligt, da er nur IP-Pakete zwischen Client und Gateway transportiert.

2.3 Securitymodelle in VPN's

Wie ich bei den Anforderungen an VPN bereits erwähnt habe, ist Security ein sehr wichtiger Bestandteil von VPN Netzen, da der Transport privater (confidential) Daten erfolgt. Aus diesem Grund muss sichergestellt werden, dass Vertraulichkeit und Integrität geschützt werden, sowie ein Schutz vor Denial-of-Service und Replay-Angriffen implementiert wird.

- *Vertraulichkeit* (Informationen dürfen nicht von dritten eingesehen werden)

- *Authentisität* (Daten dürfen nicht von falschen Absenderaddressen stammen)
- *Integrität* (Daten dürfen nicht durch dritte verändert wurden sein
- *Schutz vor wiederholtem Senden*
- *Indentifikation* (Sender und Empfänger müssen sich gegenseitig eindeutig identifizieren können)
- *Schutz vor Angriff auf das gesamte VPN-System*

Da das VPN meist nur ein Bestandteil eines Unternehmensnetzwerkes ist, muss aber gerade auch die Schnittstelle zu anderen Netzwerkbereichen mit beachtet werden. Heutzutage hat sich vorallem der Schutz auf der Netzwerkebene, also auf Level-3 des ISO/OSI Modells durchgesetzt (IPSec), aber auch auf der Transportschicht (SSL). Bervor ich auf die möglichen Verfahren genauer eingehe, möchte ich einen kurzen Überblick über die meistverwendeten Chiffrierungsalgorithmen geben.

2.3.1 Verschlüsselungsalgorithmen

Der Data Encryption Standart (DES) ist das wohl bekannteste symmetrische Verschlüsselungsverfahren. Bei symmetrischen Verfahren vereinbaren Sender und Empfänger einen Schlüssel der sowohl zum Ver- sowie Entschlüsseln verwendet wird. Bei DES wird ein 64-Bit großer Klartext mit Hilfe eines 56-Bit Schlüssels, in einen 64-Bit Chiffretext verwendet. Dieses Resultat wird in 16 Runden realisiert. In jeder Runde wird ein 48-Bit Teilschlüssel verwendet, der aus dem 56-Bit Originalschlüssel erzeugt wurden ist. Die Entschlüsselung erfolgt auf die gleiche Weise. Da DES vor über 30 Jahren entwickelt wurde, reichen die Schlüssellängen für die heutige Zeit nicht mehr aus. Daher sollten als Algorithmen eher die Triple-DES oder der Advanced Encryption Standart (AES) in Betracht gezogen werden. Das Problem bei allen symmetrischen Verfahren ist jedoch, dass sowohl dem Sender als auch dem Empfänger der Schlüssel vorliegen muss, und daher der Schlüssel in irgendeiner Form übertragen werden muss, dadurch wird ein hohes Sicherheitsrisiko verursacht, bevor mit der Verschlüsselung überhaupt begonnen wird. Bei der asymmetrischen Verschlüsselung werden im Gegensatz dazu zwei verschiedene Schlüssel verwendet. Die Verschlüsselung der Nachricht erfolgt mit einem sogenannten Public-Key. Die Entschlüsselung mit einem Privat-Key, der nur den Empfänger der Nachricht bekannt ist. Die Schlüssel werden mit Hilfe mathematicher Algorithmen erzeugt, wobei die bekanntesten Diffie-Hellman und RSA sind. RSA beruht auf der Primfaktorzerlegung einer großen Zahl. Der Hintergrund ist, dass mit den Faktoren p und q einfach die Zahl n zuerechnen ist (n=p*q), andersherum es aber fast unmöglich ist, Rückschlüsse auf p bzw. q zu ziehen. Der öffentliche Schlüssel wird durch das Tupel (n,e) gebildet, die Chiffrierung

erfolgt dann mit $C = M^e mod n$. Die Entschlüsselung ist mit dem privaten Schlüssel, durch das Tupel (n,d): $M = C^d mod n$ möglich. Die Erzeugung der Schlüsselpaare erfolgt mit Hilfe des erweiterten Euklidischen Algorithmusses. Leider würde eine genauere Behandlung der Verschlüsselungsalgorithmen den Umfang dieser Arbeit sprengen.

2.3.2 IPSEC

IPSec bietet einen umfassenden Schutz für den Datenverkehr auf IP Ebene, dabei können die Pakete mit unterschiedlichen Verfahren mit verschiedenen Schlüssellängen verschlüsselt werden. Verbreitete Verfahren sind in diesem Fall DES, Triple-DES, AES. Schutz vor Veränderung der Daten wird durch Hash-based-Message-Authentification Code erreicht, dabei handelt es sich um kryptografisch geschützte Prüfsummen, die durch Hash-Funktionen berechnet werden. Mit diesem Verfahren kann genauso die Authentizität einen Datenpaketes kontrolliert werden. Außerdem wurden in IPSec auch Vorkehrungen gegen Denial-of-Service-Angriffen, Replay-Angriffen und Man-in-the-Middle-Angriffen implementiert. Da IPSec in der Standart Variante symmetrische Schlüssel benutzt, müssen diese Sender und Empfänger vorliegen oder mit übermittelt werden.

2.3.3 IKE

Eine Möglichkeit dies zu vermeiden bietet die Kombination mit dem Internet-Key-Exchange-Protokolls (IKE). Mit diesem Protokoll können sowohl bi-direktionale ISAKMP Sicherheitsassoziaionen als auch uni-direktionale Sicherheitsassoziationen (SAs) für Sicherheitsprotokolle wie IPSec erzeugt werden. Den großen Vorteil von IKE gegenüber IPSec bildet das Schlüsselmanagement, dass außer den von IPSec verwendeten Pre-Shared-Key auch eine Authentifizierung mit Digital-Signature oder eine Public-Key-Encryption wie RSA verwendet werden kann. In den übrigen Sicherheitsanforderungen ist IKE nahezu identisch zu IPSec.

2.3.4 SSL

Wurde ursprünglich von Netscape für das HTTP Protokoll entwickelt. Die Datenverschlüsselung erfolgt mit Hilfe den vorhin vorgestellten DES Algorithmus mit 40 oder 56-bit Schlüssellänge oder den neueren AES Algorithmus. Der Unterschied zum IPSec Verfahren liegt darin, dass man die verschiedenen Verfahren für Verschlüsselung, Datenauthentifizierung und Datenintegritätsprüfung nicht frei kombinieren darf, sondern diese in sogenannten Chipher-Suites festgelegt sind. Datenintegrität und Authentizität wird

mit den gleichen Hashfunktionen wie bei IPSec erzeugt. Für das Schlüsselmanagement lässt SSL verschiedene Algorthmen wie RSA, Diffi-Hellmann und DSA zu. Ein großer Nachteil von SSL ist es, dass mit diesem Verfahren kein Schutz vor Denial of Service Angriffen möglich ist, da diese Angriffe auf IP, UDP, ICMP oder TCP abziehlen und SSL erst zum Einsatz kommt, wenn diese Schichten bereits durchlaufen wurden. Da bei SSL genauso wie bei IPSec nur eine Browserseitige Benutzerauthentifizierung möglich ist, muss diese getrennt von SSL erfolgen.

2.3.5 L2TP + IPSEC

Zum Abschluss möchte ich die Kombinationn von L2TP + IPSec erläutern, da dieses Verfahren seit Windows 2000 vom Softwareriesen Microsoft vorrangetrieben wird. IPSec kann wie vorhin erläutert nur IP Pakete Tunneln, bzw es ist schlecht für Remote Access zuverwenden, L2TP kann zwar mit Hilfe von PPP alle möglichen Protokolle Tunneln nutzten bietet aber wie schon erwähnt keine nennenswerten Sicherheitsmerkmale. Diese Einschränkungen werden mit der Kombination der beiden Verfahren beseitigt. Die Funktionsweise ist recht einfach, es wird zuerst zwischen Gateway und Client eine IPSec Verbindung aufgebaut, besteht diese wird dadurch ein L2TP Tunnel eröffnet. Dadurch können dann die PPP-Frames transportiert werden. Folgende Abbildung verdeutlicht wie dies im einzelnen Erfolgt: Zuallererst werden die IP Pakete in den PPP-Rahmen gemapt. Dieser Rahmen dann wie im L2TP Tunneling üblich in L2TP-Datenpakete gekappselt, diese anschließend in UDP/IP-Pakete. Nun kommt IPSec zur Anwendung da jetzt um die enstandenen Pakete ein IPSec-Header und Trailer konztruiert wird und somit eine Verschlüsselung erreicht und ein Message Authentification Code berechnet wird. Abschließend werden dieses Paket nochmal per PPP eingekappselt, wie durch Abbildung 10 verdeutlicht wird und anschließend verschickt.

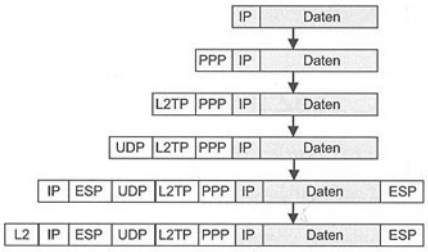

Abbildung 10: Manfred Lipp: Erzeugung L2TP/IPSec-Paketen in VPN Aufbau und Sicherheit, Seite 314

Ein großer Nachteil ist jedoch der deutlich erhöhte Datentransfer und Rechenleistung, die man bei der Kombination beider Modelle benötigt. Wie bei allen anderen VPN und NAT Techniken muss auch hier eine Kosten - Nutzen Analyse durchgeführt werden, dh. wieviel Schutz benötige ich in Abhängigkeit zum Preis.

3 Zusammenfassung

Ich habe mit dem Paper einen Überblick die Funktionsweise von Network Address Translation und Virtual Private Networks gegeben. Zusätzlich habe ich die Möglichkeiten aufgezeigt, die diese Techniken für Unternehmen, aber auch für jeden Einzelnen bieten. Unternehmen werden, wie vorhin verdeutlicht, standortunabhängiger und es wird eine deutlich größere Produktivität sowie Mobilität ermöglicht. Bei der Einführung eines VPN's sollte aber sehr genau analysiert, werden welche Variante am besten, für die eigenen Anforderungen geeignet ist und die benötigte Sicherheit gewährleistet. NAT bietet zwar eine vorübergehende Lösung des IPv4 Addressproblems, stellt aber aufgrund der bereits aufgezählten Nachteile, auf keinen Fall eine endgültige dar.

4 Literatur

Literatur

[1] Wikipedia: The Free Enzyklopedia. http://de.wikipedia.org, 2007-08-15.

[2] Stun Standard - rfc 3489 Network Working Group (J.Rosenberg, J.Weinberger)

[3] Arne Vater. Arbeitsvorlage Latex / Bibtex, SS 2007.

[4] Manfred Lipp. VPN Virtuelle Private Netzwerke - Aufbau und Sicherheit. *Addison-Wesley*, 2006.

[5] William Stallings. Internetworking with TCP/IP. *Prentice Hall*, 2006.

[6] Prof. Dr. Christian Schindelhauer. Vorlesung Systeme II, SS 2007