fhwedel
UNIVERSITY OF APPLIED SCIENCES

Seminar IT-Sicherheit

Netzwerk-Sicherheit

Name	Torben Allers
Betreuer	Prof. Dr. Gerd Beuster
Matrikelnummer	WInf9251
Fachsemester	5
Verwaltungssemester	5
Semester	Wintersemester 12/13

Inhaltsverzeichnis

1 Einleitung

Netzwerk-Sicherheit ist in den Unternehmen ein Thema von zentraler Bedeutung. Fast alle sensiblen Daten eines Unternehmens liegen in elektronischer Form vor und sind vielen Bedrohungen ausgesetzt. Zum Schutz dieser Daten reicht es heutzutage nicht mehr aus, den physischen Zugang, also den Zutritt zu Serverräumen, zu beschränken und zu überwachen, da der Zugriff auf die sensiblen Daten auch aus dem Internet erfolgen kann.

So ist es zum Beispiel im April 2011 Hackern gelungen sich mit den Kundendatenbanken der Firma Sony[1] zu verbinden und somit Zugriff auf die sensiblen Kundendaten der Firma zu erlangen. Dabei wurden Adressdaten, Passwörter und Kreditkartendaten von den Servern entwendet.

Sicherheitslücken in einem Unternehmensnetz können also großen Schaden für das Unternehmen verursachen.

Diese Seminararbeit befasst sich mit verschiedenen Techniken, mit denen die Sicherheit in Netzwerken gewährleistet und erhöht werden kann. Zum einen wird die Technik der Firewalls betrachtet, mit deren Hilfe der unautorisierte Zugriff auf ein Unternehmensnetz unterbunden werden kann. Weiter wird mit den Virtual Private Networks (VPN) eine Möglichkeit vorgestellt, mit der ein Zugriff auf das geschützte Unternehmensnetz realisiert werden kann, ohne dabei den Schutz der Firewall zu beeinträchtigen.

Darüber hinaus ist die Aufteilung eines Unternehmensnetzes in kleine Teilnetze eine weitere Maßnahme um die Netzwerk-Sicherheit zu erhöhen. Für die Umsetzung der Teilnetze werden häufig in Unternehmen virtuelle lokale Netze (VLANs) eingerichtet.

[1] Quelle [Q6]

2 Firewall

2.1 Grundgedanke von Firewalls

Das Internet ist ein Netz von Netzen verschiedenster Institutionen wie beispielsweise Unternehmen, Verbänden, Vereinen und Hochschulen. Das Netzwerk einer Institution, speziell in Unternehmen, wird auch als Intranet bezeichnet. Das Intranet ist dabei häufig mit dem Internet verbunden und über das Internet können beliebige an das Netz angeschlossene Rechner miteinander kommunizieren. Wenn also ein Rechner einen Dienst anbietet, so macht es rein technisch gesehen keinen Unterschied, ob ein PC aus dem Nachbarbüro diesen Dienst aufruft oder ob der Dienst von einem Computer aufgerufen wird, der kilometerweit entfernt an einem anderen Ort steht.

Aus der Sicherheitsperspektive gesehen gibt es gute Gründe, den Rechner im Nachbarbüro und generell alle Rechner im Netzwerk der eigenen Institution als etwas vertrauenswürdiger einzustufen:

- Die Rechner im Intranet unterliegen in der Regel den gleichen administrativen Richtlinien und Regularien
- Die Rechner im Intranet werden in der Regel durch Mitglieder derselben Institution genutzt

Somit ist also der Zugang zum Intranet im Gegensatz zum Internet bestimmten Zugangskontrollen, sowohl hinsichtlich der verwendeten Geräte als auch der Benutzer, unterworfen.

Auf Rechnern im Intranet kann es bestimmte Dienste geben, die ausschließlich für Mitglieder der Institution gedacht sind und die aus anderen Netzen als dem Intranet nicht verfügbar sein müssen. Umgekehrt kann es auf Rechnern im Internet bestimmte Dienste geben, etwa Webseiten auf bestimmten Servern, deren Abruf von Rechnern aus dem Intranet heraus unterbunden werden soll. Zusammenfassend ist es also ungeeignet, die Rechner im Intranet uneingeschränkt auf das Internet zugreifen zu lassen und umgekehrt.

Aus dieser Überlegung[2] ist die Idee der Firewall entstanden, die eine stufenweise Kontrolle darüber ermöglicht, was zwischen Inter- und Intranet und umgekehrt erlaubt ist und was nicht.

Eine Firewall sitzt an der Verbindungsstelle von Intra- und Internet und kontrolliert den Datenfluss zwischen beiden Netzen anhand festgelegter Regeln. Entsprechend dieser Regeln unterscheidet die Firewall bei der Interaktion der Netze zwischen erlaubten und unerlaubten Datenfluss und unterbindet den unzulässigen Datenverkehr. Abbildung 2.1[3] stellt diesen Sachverhalt noch einmal grafisch dar.

[2] Quelle [Q1] – Seite 157-158
[3] Quelle [A1] – Seite 159

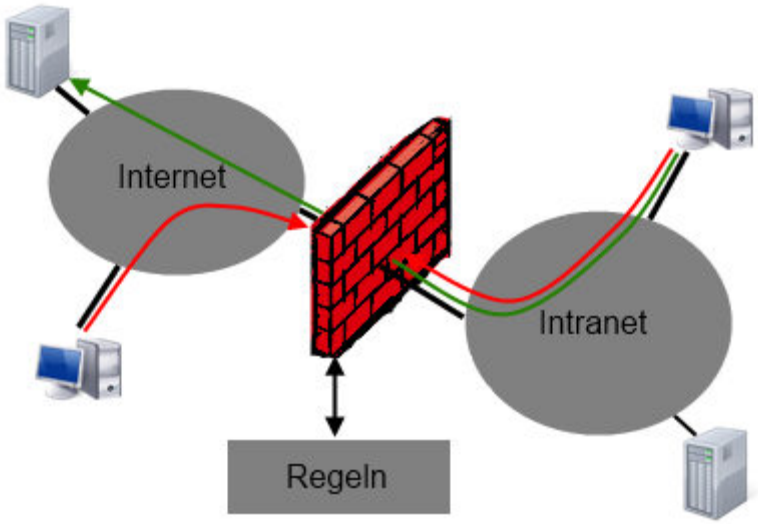


Abbildung 2.1 - Prinzip einer Firewall

2.2 Paketfilter

2.2.1 Einführung

Zeitgemäße Firewalls bestehen aus verschiedenen Komponenten. Der ursprünglichste und am weitesten verbreitete Typ ist der sogenannte Paketfilter[4]. Besonders einfache Firewalls können auch nur aus einem Paketfilter bestehen.

Typischerweise sind Paketfilter in der Zwischenstation auf Netzwerkschichtebene integriert, die das Intranet mit dem Internet verbindet, also einem Router. Da jeglicher Verkehr zwischen Intranet und Internet und umgekehrt über diesen Router läuft, kann damit sichergestellt werden, dass der gesamte Datenverkehr zwischen den Netzen auf Paketebene analysiert werden kann.

Paketfilter bestehen aus einer oder mehreren Regelketten. Jede der Regelketten besteht aus einer oder mehreren Regeln und einer Default-Aktion. Jede Regel spezifiziert dabei bestimmte mögliche Eigenschaften eines Paketes sowie eine Aktion. Wenn ein Paket die in einer Regel spezifizierten Eigenschaften besitzt, spricht man von einem Match. Der Paketfilter bearbeitet ein eingehendes Paket nach dem in der Abbildung 2.2[5] gezeigtem Schema.

Die Regeln der Regelkette werden nun in der durch die Regelkette vorgegebene Ordnung durchlaufen und es wird jeweils überprüft, ob die Regel und das Paket einen Match bilden. Ist dies der Fall, wird das Durchlaufen der Regelkette abgebrochen und die in der Regel vorgegebene Aktion ausgeführt. Mögliche Aktionen, die in einer Regel festgelegt sein können, sind das Weiterleiten des Paketes (Überprüfung des Paketes mit positivem Ergebnis abgeschlossen), das Verwerfen und Löschen des Paketes (Überprüfung des Paketes mit negativem Ergebnis abgeschlossen) oder der Sprung in eine andere Regelkette (Überprüfung des Paketes noch nicht abgeschlossen und Fortsetzung der Bearbeitung erfolgt in einer anderen Regelkette, beginnend mit der ersten Regel dieser Kette). Durchläuft das

[4] Quelle [Q1] – Seite 159 ff.
[5] Quelle [A1] – Seite 161

Paket die gesamte Regelkette, ohne einen Match mit einer Regel zu bilden, wird die für die Regelkette angegebene Default-Aktion durchgeführt.

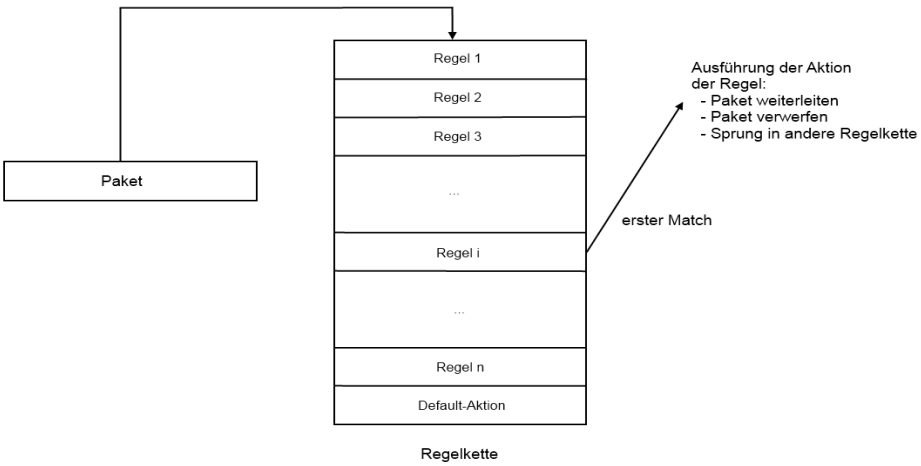


Abbildung 2.2 - Arbeitsweise eines Paketfilters

Beim Überprüfen der Datenpakete anhand der Regeln werden unter anderen folgenden Header-Informationen ausgelesen:

- IP-Quelladresse
- IP-Zieladresse
- Das eingebettete Protokoll (TCP, UDP etc.)
- TCP/UDP-Quellport
- TCP/UDP-Zielport

2.2.2 Typische Konfiguration von Paketfiltern

Es gibt zwei verschiedene Möglichkeiten, die Default-Aktion der Regelkette zu konfigurieren:

- Erlaube alles, was nicht explizit verboten ist
  Die Regeln in den Ketten spezifizieren unerwünschten Datenverkehr. Pakete, die mit einer der Regeln matchen, werden verboten. Pakete, die mit keiner der Regeln gematcht werden können, werden erlaubt. Die Pakete werden also per Default akzeptiert (Default-Accept).

- Verbiete alles, was nicht explizit erlaubt ist
  Die Regeln in den Ketten spezifizieren erlaubten Datenverkehr. Pakete, die mit einer der Regeln matchen, werden durchgelassen. Pakete, die mit keiner der Regeln gematcht werden können, gelten als unerwünscht und werden nicht weitergeleitet (Default-Deny).

Weiter ist es möglich diese beiden Techniken zu kombinieren, so dass Firewalls mit unterschiedlichen Default-Aktionen in den verschiedenen Regelketten entstehen.

Unabhängig davon welche der beiden Techniken verwendet wird, kann die gleiche Filterung erreicht werden. Jedoch ist die Default-Deny-Methode in der Regel als sicherer einzustufen, da die Pakete, auf denen keine Regel zutrifft verworfen werden.

Bei der Spezifizierung der Regeln, welche Datenpakete durchgelassen werden sollen, muss mit hoher Aufmerksamkeit vorgegangen werden, damit nicht unerwünschter Datenverkehr unbeabsichtigt die Firewall passieren kann.

Weiter ist die Reihenfolge der Regeln in einer Regelkette ein wichtiger Punkt, von der das Filterergebnis stark abhängt. Als konkretes Beispiel seien folgende zwei Regeln gegeben:

(a) Verbiete jeglichen Datenverkehr zu IP-Zieladresse x
(b) Erlaube TCP-Datenverkehr zu TCP-Zielport 80

Werden die Pakete in der Reihenfolge (a), (b) bearbeitet, so werden TCP-Segmente zu IP-Zieladresse x und TCP-Zielport 80 durch Regel (a) verworfen und Regel (b) kommt für das Paket nicht zum Einsatz.

Erfolgt die Bearbeitung aber in der Reihenfolge (b), (a), so wird das Paket durch Regel (b) durchgelassen und Regel (a) wird nicht mehr betrachtet.

2.2.3 Statische und dynamische Paketfilter

Bei den Paketfiltern wird zwischen statischen und dynamischen Paketfiltern unterschieden. Bei einem statischen Paketfilter hängt die Entscheidung des Filters, was mit einem Paket geschieht, ausschließlich von dem betrachteten Paket selbst ab. Es werden also keine anderen Informationen zur Bearbeitung herangezogen, der Paketfilter ist zustandslos. Statische Paketfilter sind einfach realisierbar, jedoch besitzen sie einige Schwächen, die anhand des folgenden Beispiels verdeutlicht werden sollen. Dieses Beispiel wird in der Quelle [Q1] auf den Seiten 163-165 noch näher betrachtet.

Es soll ermöglicht werden, dass ein Rechner im Intranet (IP-Adresse x, beliebiger TCP-Port) zu Webservern im Internet eine Verbindung aufbauen kann, um mit den Webservern über TCP und Port 80 (http) zu kommunizieren. Bei diesem Beispiel wird von einem Default-Deny in der konsultierten Regelkette ausgegangen.

Um dies zu ermöglichen, müssen alle TCP-Segmente mit den Regeln der konsultierten Regelkette der Firewall matchen, so dass folgende zwei Regeln benötigt werden:

(a) Erlaube TCP-Segmente von IP-Quelladresse x, TCP-Quellport beliebig zu beliebigen Rechnern im Internet auf TCP-Zielport 80.
(b) Erlaube TCP-Segmente von beliebigen Rechnern im Internet von TCP-Quellport 80 zu IP-Zieladresse x, TCP-Zielport beliebig.

Diese beiden Regeln sind jedoch zu grob strukturiert und öffnen eine Sicherheitslücke. Ein Angreifer irgendwo im Internet könnte von TCP-Port 80 aus versuchen, eine TCP-Verbindung zu einem beliebigen Port auf Rechner x aufzubauen. Die Firewall würde diesen Versuch eines Verbindungsaufbaus aufgrund von Regel (b) erlauben und es dem Angreifer so ermöglichen, eine TCP-Verbindung mit einem beliebigen Port auf dem Rechner x herzustellen.

Es muss also verhindert werden, dass Verbindungen vom Internet ins Intranet aufgebaut werden können, wobei der umgekehrte Weg, also Verbindungen vom Intranet ins Internet, möglich sein sollen.

Bei der Verwendung von TCP kann dies mit einem statischen Paketfilter tatsächlich realisiert werden, indem weitere Merkmale der TCP-Segmente während des Verbindungsaufbaus betrachtet werden. Der Verbindungsaufbau bei TCP zwischen Client und Server erfolgt über den Three-Way-Handshake. Das erste TCP-Segment, welches vom Client an den Server gesendet wird, besitzt ein gesetztes SYN-Flag, das ACK-Flag ist jedoch nicht gesetzt. Durch diese Konstellation von SYN-Flag und ACK-Flag wird das erste TCP-Segment bei einem Verbindungsaufbau eindeutig identifiziert. Um nun den Verbindungsaufbau vom Internet ins Intranet zu unterbinden, muss die Regelkette um folgende Regel erweitert werden.

(a) Verbiete TCP-Segmente von beliebigen Rechnern im Internet von TCP-Quellport 80 zu IP-Zieladresse x, TCP-Zielport beliebig, wenn das SYN-Flag gesetzt ist, das ACK-Flag aber nicht.
(b) Erlaube TCP-Segmente von IP-Quelladresse x, TCP-Quellport beliebig zu beliebigen Rechnern im Internet auf TCP-Zielport 80.
(c) Erlaube TCP-Segmente von beliebigen Rechnern im Internet von TCP-Quellport 80 zu IP-Zieladresse x, TCP-Zielport beliebig.

Abbildung 2.3[6] soll dieses Verhalten noch einmal veranschaulichen.

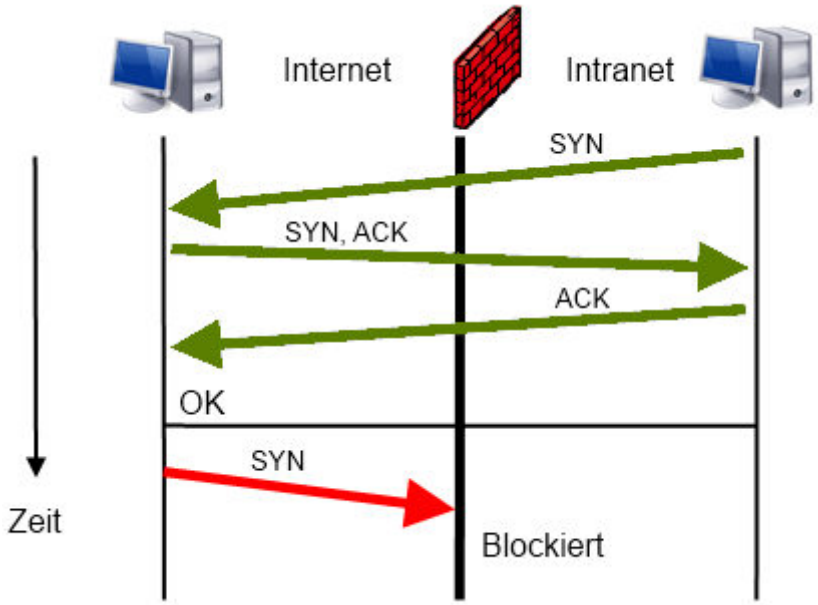


Abbildung 2.3 - TCP-Verbindungsaufbau

Mit dieser Konfiguration ist es nun unmöglich eine TCP-Verbindung aus dem Internet ins Intranet aufzubauen. Doch es bleiben weitere Sicherheitslücken bestehen, die nicht mit einem statischen Paketfilter beseitigt werden können. So existiert nach dem Verbindungs-

[6] Quelle [A1] – Seite 163

aufbau kein Unterschied mehr zwischen Client und Server. Dadurch kann nach dem Aufbau der Verbindung anhand eines einzelnen TCP-Segments nicht mehr festgestellt werden, wer die Verbindung aufgebaut hat oder ob überhaupt ein Verbindungsaufbau stattgefunden hat.

Dies kann ein Angreifer nun wieder wie folgt ausnutzen. Von einem beliebigen mit dem Internet verbundenen Rechner aus könnte er, ohne dass tatsächlich eine TCP-Verbindung aufgebaut wurde, ein TCP-Segment ohne gesetztes SYN-Flag fälschen. Dieses TCP-Segment wird dann von Port 80 des Rechners aus an einen beliebigen Port auf Rechner x gesendet. Die Firewall würde dieses Segment nach den oben definierten Regeln durchlassen. Zwar besteht zwischen dem Rechner des Angreifers und dem Rechner x im Intranet keine TCP-Verbindung, aber der Rechner x könnte mit einer entsprechenden Fehlermeldung reagieren, die dem Angreifer Rückschlüsse auf das Intranet erlaubt. Auch eine Beeinträchtigung der Funktion des Rechners x ist denkbar.

Auf so eine Art von Angriff bietet der statische Paketfilter keinen Schutz mehr.

Wenn bei der Kommunikation statt einer TCP-Verbindung eine UDP-Verbindung verwendet wird, bietet ein statischer Paketfilter keinen Schutz, da bei der UDP-Verbindung kein Verbindungsaufbau erfolgt. Dadurch ist keine Konfiguration des statischen Paketfilters möglich, die Verbindungen aus dem Intranet ins Internet erlauben und Verbindungen aus dem Internet ins Intranet verbieten, da es keine Identifikationsmöglichkeit des ersten ausgetauschten Datenpaketes gibt.

Dieser Sachverhalt hat dazu geführt, dass heute in der Praxis hauptsächlich dynamische Paketfilter zum Einsatz kommen. Bei einem dynamischen Paketfilter kann die Entscheidung des Filters, wie mit einem Datenpaket verfahren werden soll, von vorangegangen Paketen abhängen. Der dynamische Paketfilter ist zustandsbehaftet. In der Praxis registrieren die meisten dynamischen Paketfilter den Aufbau einer TCP-Verbindung oder das erste UDP-Datenpaket, welches zwischen zwei Rechnern ausgetauscht werden soll und treffen anhand dieses Paketes eine Entscheidung, ob diese Verbindung bzw. der Datenfluss erlaubt oder unerwünscht ist. Diese Entscheidung wird dann auch auf alle danach eintreffenden Pakete der Verbindung oder des Datenflusses angewendet. Durch diese Technik ist das Fälschen von Datensegmenten zum Überwinden der Firewall nicht mehr ohne weiteres möglich. Entsprechende Regeln, um Verbindungen vom Intranet ins Internet über http (und sonst nichts) zu erlauben, könnten daher lauten:

(a) Erlaube neue TCP-Verbindungen von IP-Quelladresse x, TCP-Quellport beliebig zu beliebigen Rechnern im Internet, TCP-Zielport 80.
(b) Erlaube beliebige Pakete, die zu einer bereits bestehenden Verbindung gehören.
(c) Verwirf alle anderen Pakete.

Die folgende Tabelle 2.1 stellt die Eigenschaften von statischen und dynamischen Paketfiltern gegenüber.

Eigenschaft	Statischer Paketfilter	Dynamischer Paketfilter
Charakteristik	Die Entscheidung des Filters, was mit einem Paket geschieht, hängt nicht von vorangegangenen Paketen ab (zustandslos).	Die Entscheidung des Filters, was mit einem Paket geschieht, kann von vorangegangenen Paketen abhängen (zustandsbehaftet).
Möglichkeiten UDP	Kann bei UDP-Datenflüssen nicht unterscheiden, ob das erste Paket vom Intranet ins Internet ging oder umgekehrt.	Kann bei UDP-Datenflüssen unterscheiden, ob das erste Paket vom Intranet ins Internet ging oder umgekehrt.
Möglichkeiten TCP	Gefälschte TCP-Segmente von außen können einfach durch die Firewall gelangen und so Sicherheitslücken öffnen, da keine Information über bestehende Verbindungen vorliegt.	TCP-Segmente, die nicht zu existierenden, erlaubten Verbindungen gehören, werden verworfen.
Umsetzung	Sehr einfach, da keine Information über vorangegangene Pakete oder Verbindungen gespeichert werden muss.	Komplizierter, da Information über vorangegangene Pakete oder Verbindungen gespeichert werden muss.

Tabelle 2.1 - Eigenschaften statischer und dynamischer Paketfilter

2.3 Application-Level-Gateway

Application-Level-Gateways[7] (in der Praxis besser bekannt unter dem Namen Proxy-Server) überwachen den Datenverkehr zwischen zwei Netzen auf der Applikationsschichtebene. Dies hat den Vorteil, dass hier die vollständigen Protokoll- und Nutzlastinformationen des jeweiligen Applikationsprotokolls vorliegen. Dadurch ist eine detaillierte Analyse dieser Informationen hier möglich. Allerdings ist die konkrete Arbeitsweise eines Application-Level-Gateway stark von der jeweiligen Anwendung abhängig, da der Datenverkehr auf der Anwendungsebene kontrolliert wird.

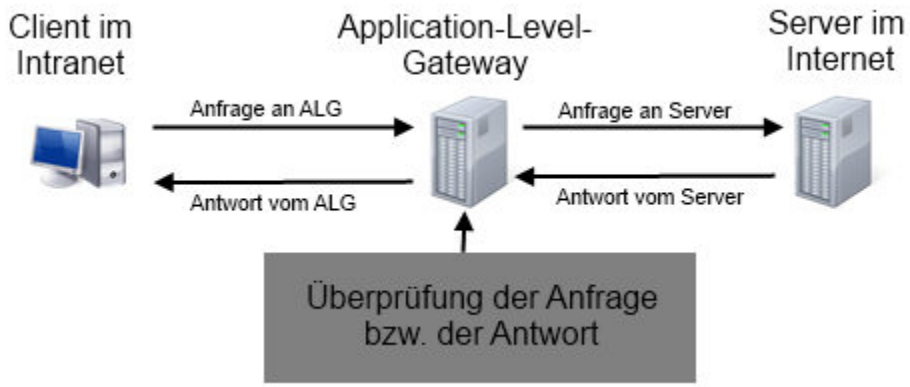
Der Grundgedanke hinter Application-Level-Gateways besteht darin die Verbindungen zwischen den Stationen im Internet und im Intranet nicht direkt zu erstellen, sondern sie über eine Zwischenstation laufen zu lassen. Diese Zwischenstation überwacht, analysiert und filtert den Informationsaustausch auf der Applikationsebene. Dabei sind wieder Regeln festgelegt, mit denen erwünschte und unerwünschte Aktionen und Funktionen der Applikation definiert werden.

[7] Quelle [Q1] – Seite 179 ff.

Die Kommunikation zwischen einem Client im Intranet und einem Server im Internet verläuft dann wie folgt ab:

- Der Client stellt eine Anfrage an das Application-Level-Gateway.
- Das Application-Level-Gateway überprüft und analysiert die Anfrage auf Zulässigkeit und Sicherheitsrelevanz.
- Ist die Anfrage vom Client erlaubt, stellt das Application-Level-Gateway die Anfrage entweder entsprechend bestehender Regeln verändert oder unverändert dem Server im Internet zu.
- Das Application-Level-Gateway empfängt die Antwort des Servers. Diese wird ebenfalls überprüft und analysiert.
- Ist die Antwort des Servers zulässig, wird sie vom Application-Level-Gateway anhand bestehender Regeln entweder verändert oder unverändert an den Client weitergeleitet.

Abbildung 2.4[8] stellt dieses Szenario noch einmal grafisch dar.



2.4 - Application-Level-Gateway

Bei der Überprüfung kann der Inhalt des Informationsaustausches unter anderem auf das Auftreten von Schlüsselwörtern im Inhalt oder auf Malware untersucht werden. Weiter kann über Listen und Indexdienste ermittelt werden, ob der angesprochene Kommunikationspartner bestimmten vorgegebenen Kriterien entspricht. So ist zum Beispiel denkbar bestimmte Domains in ihrer Erreichbarkeit zu beschränken.

Neben den Sicherheitsfunktionen können Application-Level-Gateways auch noch andere Funktionen erfüllen. So ist zum Beispiel das Caching von durch Applikationen häufig angefragten Daten eine weitere Funktion eines Application-Level-Gateways. Dadurch kann ein schnellerer Zugriff auf diese Daten gewährleistet werden.

Application-Level-Gateways werden meistens in Verbindung mit einem oder mehreren Paketfiltern eingesetzt. Der Paketfilter kann dann so konfiguriert werden, dass die Anwendungen tatsächlich über das Application-Level-Gateway laufen, indem direkte Verbindungen durch entsprechende Regeln untersagt werden.

[8] Quelle [A1] – Seite 180

2.4 Demilitarized Zone

Die Demilitarized Zone[9] ist eine Sicherheitszone, in der die extern verfügbaren Server, wie zum Beispiel E-Mail-Server oder Webserver mit dem Internetauftritt eines Unternehmens, und die Application-Level-Gateways betrieben werden.

Diese Zone befindet sich zwischen dem Internet und dem geschützten internen Netz und ist abgesichert durch zwei Paketfilter. Der eine Paketfilter befindet sich an dem Übergang vom Internet in die Demilitarized Zone und der andere Paketfilter sichert den Übergang von der Demilitarized Zone in das geschützte interne Netz. Abbildung 2.5[10] veranschaulicht den Aufbau dieser Firewallstruktur.

Die Regeln für die beiden Paketfilter erlauben dabei den notwendigen Datenverkehr zwischen den Rechnern in der Demilitarized Zone und dem Internet sowie den Computern im geschützten internen Bereich und den Rechner in der Demilitarized Zone.

Andere Zugriffe, wie zum Beispiel nicht notwendige Zugriffe von der Demilitarized Zone auf den geschützten internen Bereich oder der direkte Zugriff von dem Internet auf den geschützten internen Bereich werden unterbunden.

Sollte ein Angreifer Zugriff auf einen Server in der Demilitarized Zone erlangen, wird durch diese Firewallstruktur der unmittelbare Zugriff auf den geschützten internen Bereich verhindert. Dieser Zugriff wird durch den zweiten Paketfilter zwischen der Demilitarized Zone und dem geschützten internen Netz unterbunden.

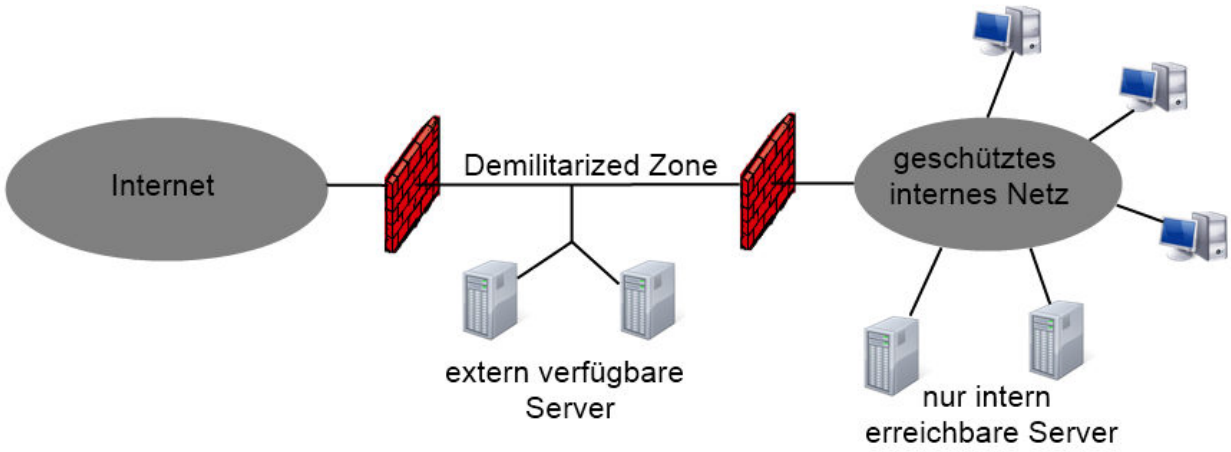


Abbildung 2.5 - Firewallstruktur mit Demilitarized Zone

[9] Quelle [Q1] – Seite 183 ff.
[10] Quelle [A1] – Seite 185

3 Virtual Local Area Network

3.1 Einführung

Ein Virtual Local Area Network[11] (VLAN) unterteilt ein bestehendes physisches Netzwerk in mehrere logische Teilnetzwerke. Dadurch besteht die Möglichkeit die Rechner der verschiedenen Abteilungen eines Unternehmens wie zum Beispiel die Forschungs- und Entwicklungsabteilung, den Vorstand oder die Personalabteilung in separaten, voneinander getrennten Netzen zu betreiben und die Kommunikation zwischen diesen Teilnetzen mit der Hilfe von Firewalls zu steuern.

Die Firewall kann also nicht nur an der Schnittstelle vom Internet ins Intranet eingesetzt werden, sondern auch innerhalb des Intranets für die Aufstellung weiterer Zugriffsrichtlinien. So kann beispielsweise der Zugriff von einer Station im Netz der Personalabteilung auf das Netz der Forschungs- und Entwicklungsabteilung unterbunden werden.

3.2 Technische Realisierung von VLANs

Für die Einrichtung eines VLAN wird zunächst ein VLAN-fähiger Switch benötigt. Die Ports dieses Switches können dann so konfiguriert werden, dass sie genau zu einem VLAN gehören. Diese technische Umsetzung wird auch als portbasiertes VLAN bezeichnet.

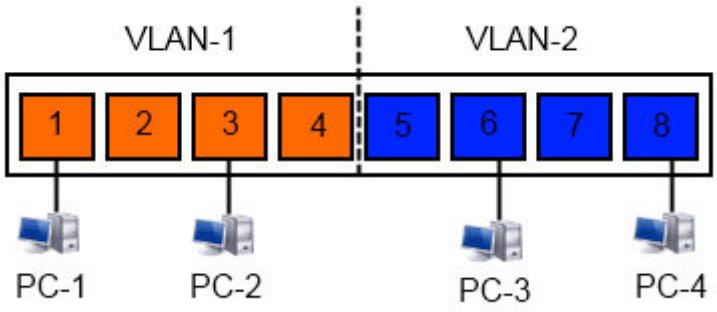


Abbildung 3.1 – Switch mit 2 portbasierten VLANs

Der in Abbildung 3.1[12] dargestellte Switch A wurde logisch in zwei VLANs (VLAN-1 und VLAN-2) aufgeteilt. Obwohl alle 4 PCs physisch an dem Switch angeschlossen sind, kann auf Grund der VLAN-Konfiguration der Datenaustausch nur zwischen PC-1 und PC-2 sowie PC-3 und PC-4 stattfinden. Die beiden VLANs können also in dieser Situation jeweils 4 Arbeitsstationen aufnehmen. In den meisten Unternehmen ist so eine Konstellation eher selten vorgesehen. Es ist außerdem denkbar, dass die Computer, welche in einem VLAN zusammengefasst werden sollen, in unterschiedlichen Räumen und auf unterschiedlichen Etagen stehen und somit große Längen von Kabel zu diesem einen Switch verlegt werden müssten. Um dies zu vermeiden, können mehrere Switche miteinander verbunden werden.

[11] Quelle [Q4] – Seite 363 ff. und [Q5]
[12] Quelle [A2]

Angenommen es gibt einen zweiten Switch B mit der gleichen Konfiguration und der gleichen Anzahl an angeschlossenen Computern wie in Abbildung 3.1. Zwei der PCs von Switch B sollen in das VLAN-1 von Switch A zugeteilt werden und die anderen beiden PCs sollen in das VLAN-2 von Switch A integriert werden.

Um diese beiden Switche miteinander zu verbinden, gibt es zwei Möglichkeiten. Zum einen ist es möglich die beiden Switche mit zwei Kabeln zu verbinden. Dabei verläuft das eine Kabel von dem VLAN-1-Bereich von Switch A in den VLAN-1-Bereich von Switch B, also zum Beispiel von Port 2 von Switch A zu Port 4 von Switch B. Das zweite Kabel wird analog zwischen den beiden VLAN-2-Bereichen der Switche verlegt, zum Beispiel von Port 5 von Switch A zu Port 5 auf Switch B. Dadurch ist die gewünschte Kommunikation der vier Computer gewährleistet.

Zum anderen können die beiden Switche über einen einzigen Port verbunden werden, so dass dieser Port von beiden VLANs genutzt werden kann. Diese Realisierungsart wird als tagged VLAN bezeichnet und ist in Abbildung 3.2[13] dargestellt.

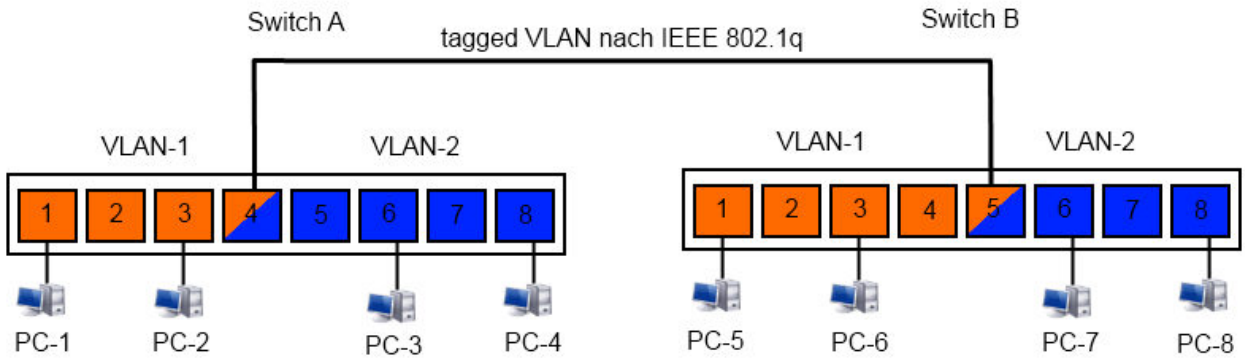


Abbildung 3.2 - tagged VLAN

Die Kommunikation zwischen den beiden Switchen erfolgt also über Port 4 von Switch A und Port 5 von Switch B. Diese beiden Ports werden als Trunk-Ports bezeichnet. Da nun der gesamte Datenverkehr der beiden VLANs über diese eine Verbindung verläuft, müssen die Datenpakete eindeutige identifiziert werden können, um sie dem entsprechenden VLAN zuordnen zu können. Diese Identifikation der Datenpakete wird durch den sogenannten VLAN-Tag, welcher im Ethernet Frame eingefügt wird und nach IEEE 802.1q definiert ist. Danach wird jedem VLAN eine eindeutige ID vergeben und diese von dem Switch in den Ethernet Frame eingefügt, so dass das Datenpaket eindeutig zu einem VLAN zugeordnet werden kann.

[13] Quelle [A2]

4 Virtual Private Network

4.1 Einführung

Mit den, unter Kapitel 2 betrachteten, Firewalltechniken können Zugriffe auf das Intranet aus dem Internet verhindert werden und somit die Ressourcen im Intranet geschützt werden. Dieses Szenario, also der Zugriff aus dem Internet auf das Intranet, ist allerdings manchmal erwünscht. Beispielsweise für Außendienstmitarbeiter oder für Mitarbeiter, die von zu Hause aus im Home Office arbeiten möchten. Diese Personengruppen können sich aber auf Grund der Firewall nicht über das Internet mit dem Intranet verbinden. Der Zugriff auf das Intranet vom Internet aus wird auch als Remote-Access, auch RAS, bezeichnet.

Das Virtual Private Network[14], auch VPN, stellt eine Technik dar, welche dieses Szenario realisiert. Ein VPN ermöglicht also das Betreiben einer sicheren, scheinbar direkten Punkt-zu-Punkt-Verbindung zwischen zwei Stationen unter Verwendung des Internets als Verbindungsmedium. Diese Verbindung kann so interpretiert werden, als wenn eine direkte Leitung zwischen den beiden Stationen existieren würde.

Beim Aufbau des VPNs erfolgt eine Authentifikation, so dass nur autorisierte Benutzer über das VPN Zugriff erhalten können. Bei der Datenübertragung über die VPN-Verbindung ist sicherzustellen, dass die Vertraulichkeit (keine Weitergabe der Daten an Dritte), Integrität (keine Veränderung der Daten) und die Authentizität (Nachweis der Echtheit der Identität des Kommunikationspartners) der Daten gewährleistet ist.

Es gibt verschiedene Arten von VPNs

- End-to-Site
  Verbindung von einem externen Rechner, wie zum Beispiel der Computer des Außendienstmitarbeiters, mit dem Intranet eines Unternehmens.
- Site-to-Site
  Verbindung von mehreren Netzen verschiedener Standorte, wie zum Beispiel der Zusammenschluss von Unternehmensnetzen.
- End-to-End
  Verbindung von mehreren Rechnern, wie zum Beispiel eine sichere Verbindung von einem Computer zu einem Buchungsserver einer Bank.

In den folgenden Abschnitten sollen die VPN-Arten End-to-Site und Site-to-Site näher betrachtet werden.

4.2 End-to-Site VPN

Die Abbildung 4.1[15] zeigt eine mögliche technische Realisierung eines End-to-Site VPNs.

Der Mitarbeiter Max Mustermann möchte einen Zugriff über das Internet auf das Intranet der Musterfirma GmbH erhalten. Die Musterfirma GmbH bietet seinen Mitarbeitern die Möglichkeit, über die in Abbildung 4.1 dargestellte VPN-Struktur, auf das Intranet zuzugreifen.

[14] Quelle [Q1] – Seite 193 ff.
[15] Quelle [A1] – Seite 195

Der Computer M von Max Mustermann besitzt über die IP-Adresse x einen Internetzugang. Weiter ist auf M eine spezielle Software installiert, der VPN-Client, der über das Internet mit dem VPN-Server S der Musterfirma GmbH eine Verbindung aufbaut. Der VPN-Server besitzt die IP-Adresse y und befindet sich in der Demilitarized Zone der Musterfirma GmbH. Diese Struktur ist häufig in der Praxis umgesetzt.

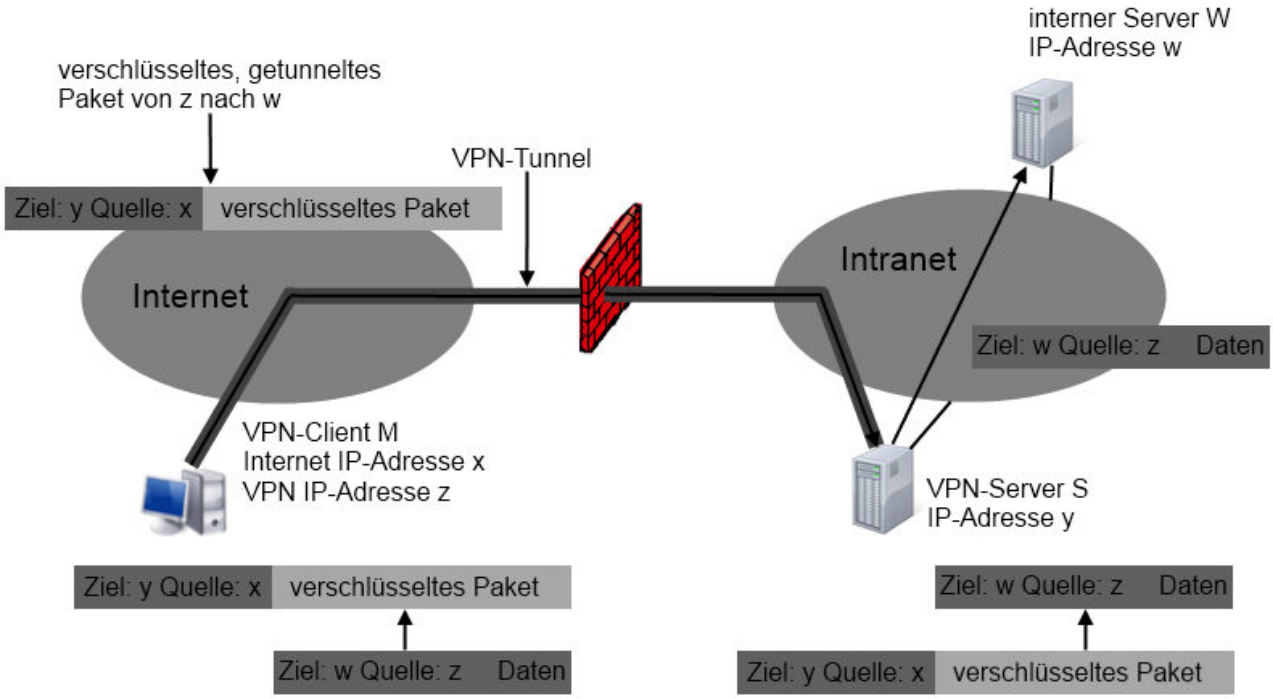


Abbildung 4.1 – End-to-Site VPN

Der VPN-Client authentifiziert sich und es werden Schlüssel vereinbart, mit denen die Kommunikation zwischen VPN-Client und dem VPN-Server kryptographisch geschützt wird. Zusätzlich zu seiner eigentlichen Internet IP-Adresse x wird dem Computer M beim Aufbau der VPN-Verbindung eine zusätzliche IP-Adresse z aus dem Adressbereich des Intranets der Musterfirma GmbH zugewiesen. Alle Anwendungen auf dem Rechner verwenden ausschließlich diese Adresse z für die Kommunikation über das Netzwerk und befinden sich so virtuell im Intranet der Musterfirma GmbH. Die VPN-Client-Software auf dem Computer M nimmt die von den Anwendungen eingehenden Pakete entgegen und tunnelt diese Pakete verschlüsselt an den VPN-Server. Dafür wird die eigentliche IP-Adresse x des Rechners verwendet.

Das Tunneln stellt dabei ein „Verpacken“ von Protokolldaten eines Protokolltyps a in Protokolleinheiten des Protokolltyps b dar. Das zu sichernde IP-Paket wird komplett in ein neues IP-Paket eingekapselt, mit einem zusätzlichen IP-Header versehen und zwischen den Systemen getunnelt. IP-Quell- und IP-Zieladresse des neuen Headers sind die durch das VPN verbundenen Systeme. Die geschützten Pakete werden dann via IP zwischen diesen Systemen befördert und auf der anderen Seite des Tunnels wieder entpackt und dann weiterbehandelt.

Möchte nun der Computer M mit dem Server W mit der zugehörigen IP-Adresse w im Intranet der Musterfirma GmbH kommunizieren, entsteht durch ein Anwendungsprogramm auf M ein Paket mit der IP-Quelladresse z und IP-Zieladresse w. Dieses Paket wird nach Anwendung kryptografischer Methoden zur Verschlüsselung und Gewährleistung der Integrität als Nutzlast vollständig in ein neues IP-Paket eingekapselt (Vorgang des Tunnelns).

Dieses neue IP-Paket enthält als IP-Quelladresse die eigentliche Internet-Adresse x des Computers M und ist an den VPN-Server gerichtet, besitzt also die IP-Zieladresse y. Der VPN-Server empfängt dieses Paket, entschlüsselt, überprüft und entkapselt es und leitet dann das ursprünglich von der Anwendung erzeugte Paket mit IP-Quelladresse y und Zieladresse an den internen Server W weiter.

Der VPN-Tunnel ist für den Server W vollkommen transparent. Er erhält ein Paket von der IP-Adresse z, an die er auch wieder antwortet. Dieses Paket nimmt der VPN-Server S entgegen und tunnelt es analog wie oben beschrieben an M weiter, wo die VPN-Software, die Entschlüsselung, Überprüfung und Entkapselung übernimmt.

4.3 Site-to-Site VPN

Zwischen dem Site-to-Site VPN und dem unter 4.2 beschrieben End-to-Site VPN gibt es konzeptionell keine großen Unterschiede. Der einzige Unterschied besteht darin, dass bei einem Site-to-Site VPN zwei Gateways durch das VPN verbunden sind.

Ein mögliches Beispiel eines Site-to-Site VPNs ist in Abbildung 4.2[16] dargestellt.

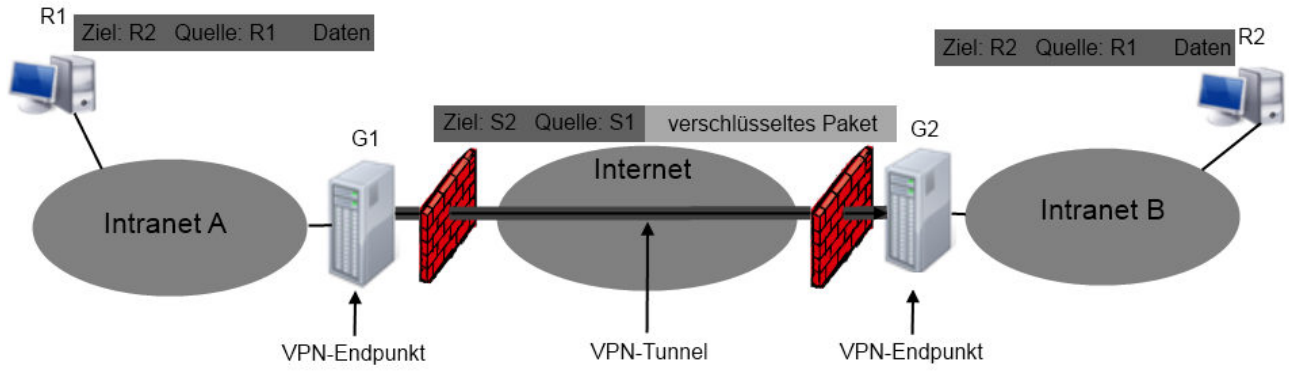


Abbildung 4.2 - Site-to-Site VPN

Wenn also Pakete von Rechner R1 in Intranet A zu Rechner R2 in Intranet B geschickt werden sollen, so werden die Pakete im Intranet A von R1 zu Gateway G1 gesendet. Gateway G1 verschlüsselt diese Pakete, kapselt sie ein und schickt sie durch das VPN über das öffentliche Internet an das Gateway G2. Dort werden die Pakete entschlüsselt und im Intranet B zu R2 weitergeleitet. Die jeweiligen Endpunkte wissen nichts von dem bestehenden VPN.

[16] Quelle [A1] – Seite 197

Umgekehrt läuft der Prozess analog ab. Im Falle eines solchen VPNs zwischen zwei Gateways erfolgt der Aufbau des VPNs auch zwischen diesen Gateways. Die Gateways benutzen dann das aufgebaute VPN wie eine private dedizierte Leitung untereinander und leiten über diese Verbindung Pakete weiter.

Aufgrund der Einkapselung, Verschlüsselung und des Tunnelns der Pakete kann ein Angreifer, der die Pakete mitlesen kann, nicht allzu viele Informationen aus dem Datenverkehr entnehmen. Insbesondere lassen sich auch die IP-Adressen der eigentlichen Endpunkte der Kommunikation, R1 und R2, nicht erkennen.

Die beiden vorgestellten VPN-Arten End-to-Site und Site-to-Site sind in der Quelle [Q1] auf den Seiten 195-198 näher erläutert.

Zusammenfassend bietet der Einsatz von VPN folgende Vorteile:
- geringere Unterhaltskosten durch Nutzung des Internets anstatt angemietete Leitungen
- beliebige Erweiterbarkeit unter Erhaltung vorhandener Teilnetzstrukturen → Flexibilität
- vorhandene Internet-Hardware kann verwendet werden, um ein VPN aufzubauen

Bei der Verwendung der beiden vorgestellten VPN-Arten ist jedoch zu beachten, dass die Daten nicht End-to-End verschlüsselt sind, sondern nur auf der durch das VPN abgesicherten Teilstrecke. In dem Beispiel aus Abbildung 4.2 sind die Daten nur zwischen G1 und G2 verschlüsselt, nicht aber zwischen R1 und G1 oder G2 und R2. Für das Versenden von vertraulichen Informationen über VPN sollte daher eine zusätzliche Verschlüsselung der Daten vorgenommen werden.

4.4 IPsec – IP Security Protocol

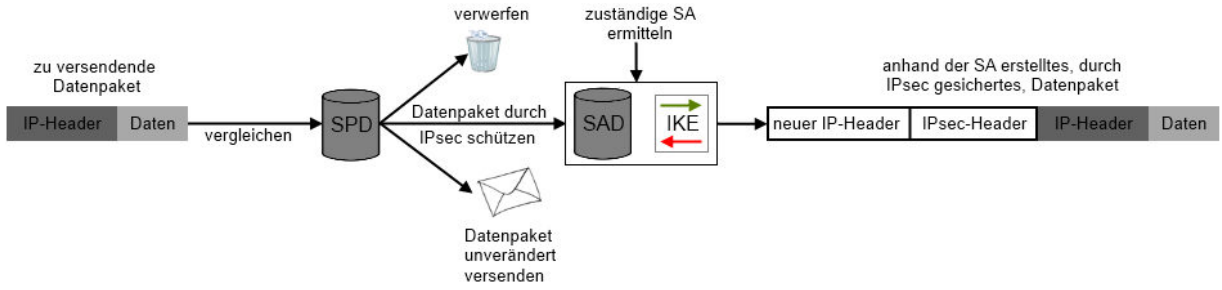
IPsec[17] ist ein wichtiges Protokoll mit dem sich ein VPN zwischen zwei Stationen realisieren lässt und beschreibt die Bereitstellung von Sicherheitsdiensten auf der IP-Schicht. IPsec arbeitet verbindungslos und wurde ursprünglich für IPv6 entwickelt. Mittlerweile ist aber auch IPsec mit IPv4 anwendbar. IPsec gewährleistet die Authentizität, Integrität und die Vertraulichkeit der versendeten Datenpakete.

Bei der Kommunikation über IPsec spielen folgende Komponenten eine Rolle:

- Betriebsmodus (Tunnel- oder Transportmodus)
- Security Association (SA) und Security Association Database (SAD)
- Security Policy Database (SPD)
- Sicherheitsprotokolle (ESP-, AH-Protokoll)

Im Folgenden werden die einzelnen Elemente und ihre Interaktion untereinander näher beschrieben, um die unter Punkt 4.2 und 4.3 vorgestellten VPN-Arten mit IPsec realisieren zu können. Abbildung 4.3 zeigt das Zusammenspiel der Komponenten grafisch auf.

[17] Quelle [Q1] – Seite 198 ff.



4.3 - Ablauf des IPsec-Protokolls

4.4.1 Betriebsmodus

IPsec kann unter zwei verschiedenen Betriebsmodi, dem Tunnelmodus und dem Transportmodus, verwendet werden.

Beim Einsatz des Tunnelmodus wird das komplette zu versendende Datenpaket, also IP-Header und Nutzdaten, gesichert und in ein weiteres IP-Paket eingebettet, um es anschließend zu versenden. Zusätzlich wird ein IPsec-Header, welcher unter anderem das verwendete Sicherheitsprotokoll beinhaltet, zwischen dem neuen IP-Header und dem ursprünglichem Datenpaket eingefügt. In dem Beispiel zum Ablauf des IPsec-Protokolls aus Abbildung 4.3 wird der Tunnelmodus verwendet. In der Praxis wird der Tunnelmodus bei VPNs der Art End-to-Site und Site-to-Site verwendet.

Der Transportmodus wird in der Praxis verwendet, um die VPN-Art End-to-End zu realisieren. Hierbei werden, im Gegensatz zum Tunnelmodus, nur die Nutzdaten durch IPsec gesichert. Auch hier wird ein zusätzlicher IPsec-Header zwischen dem IP-Header und den Nutzdaten integriert, welcher auf das verwendete Sicherheitsprotokoll schließen lässt.

4.4.2 Security Association und Security Association Database

Die Grundlage für IPsec bilden die Security Association (SA). Unter dem Konzept der SA versteht man eine Sicherheitsstrategie, die bei den kommunizierenden IPsec-Endsystemen über den Einsatz der anzuwendenden Verschlüsselungsverfahren und Schlüssel informiert. Eine SA arbeitet immer unidirektional, betrifft also nur Pakete in eine Richtung, nicht aber in die umgekehrte Richtung. Dadurch gibt es für den bidirektionalen Datenverkehr also immer mindestens eine eingehende (Inbound SA) und eine ausgehende (Outbound SA). Für den Transport von Paketen mit unterschiedlichen Sicherheitsstufen, können auch mehrere SAs über eine Verbindung existieren.

Die unterschiedlichen SAs und ihre jeweiligen Konfigurationen werden in einer Datenbank, der Security Association Database (SAD), gespeichert. Jede SA kann eindeutig anhand folgender drei Parameter identifiziert werden:

- IP-Zieladresse
- Verwendetes Sicherheitsprotokoll (AH oder ESP)
- Security Parameter Index (SPI)
  Hierbei handelt es sich um einen 4 Byte-Wert, der dazu dient, auch verschiedene SAs mit gleicher Zieladresse und gleichem Sicherheitsprotokoll unterscheiden zu können.

Ist in der SAD kein passender Eintrag für die zu verwendete SA vorhanden, kann dynamisch eine SA durch Verwendung des Internet Key Exchange Protkolls (IKE) geschaffen werden. Dabei werden mit dem Kommunikationspartner Sicherheitsparameter und Schlüssel ausgetauscht. Durch die Konfiguration der SA ist vorgegeben, wie das Datenpaket für den Transport mit IPsec gesichert werden soll.

4.4.3 Security Policy Database

Die Sicherheitsstrategie oder Security Policy in IPsec legt fest, welche Dienste auf ein- oder ausgehende Pakete anzuwenden sind. Die Regeln, aus denen sich diese Strategie zusammensetzt, sind in einer speziellen Datenbank, der Security Policy Database (SPD) abgelegt. Diese Datenbank ähnelt der Regelkette einer Firewall und funktioniert auch ganz analog. Es lassen sich sogenannte Selektoren angeben, welche den Regeln in den Regelketten einer Firewall ähnlich sind. Diese Selektoren können unter anderem die Quell- und Zieladresse der IP-Pakete sein.

Für alle eingehenden und ausgehenden IP-Pakete konsultiert IPsec die SPD-Datenbank, um zu bestimmen, wie mit dem Paket zu verfahren ist. Jeder Eintrag enthält Selektoren und bestimmt, wie mit einem matchenden Paket verfahren wird. Hierbei gibt es drei Möglichkeiten:

- Das Paket wird verworfen und gelöscht (discard)
- Das Paket wird unverändert durchgelassen (bypass)
- Das Paket wird durch IPsec umgeformt und geschützt (apply)

Bei der letzten der drei Möglichkeiten (apply) enthält die SPD einen Eintrag, durch welche SA das Paket geschützt wird und einen entsprechenden Verweis in die SAD.

4.4.4 Die Sicherheitsprotokolle AH und ESP

Die Authentizität, die Integrität und die Vertraulichkeit der versendeten Datenpakete werden durch die Sicherheitsprotokolle Authentication Header (AH) und Encapsulating Security Protocol (ESP) gewährleistet. Der Unterschied der beiden Protokolle besteht darin, dass das AH-Protokoll die Eigenschaften Authentizität und Integrität realisiert, wobei das ESP-Protokoll zusätzlich das Merkmal Vertraulichkeit der Datenpakete verwirklicht.

Für die Sicherstellung der Datenintegrität und der Authentizität wird von dem Absender eine Prüfsumme aus dem IP-Header und den Nutzdaten berechnet. Diese Prüfsumme wird an Hand eines Schlüssels ermittelt, welcher sowohl dem Absender als auch dem Empfänger des Paketes bekannt ist und zuvor über das IKE-Protokoll ausgetauscht wurde. Die ermittelte Prüfsumme wird anschließend in den AH-Header geschrieben, welcher wiederum zwischen IP-Header und Nutzdaten im IP-Paket platziert wird. In Abbildung 4.3 ist dies durch den IPsec-Header dargestellt.

Der Empfänger des Paketes kann anhand der im Header stehenden Prüfsumme und des gemeinsamen Schlüssels ebenfalls die Prüfsumme berechnen und mit der im AH-Header empfangenen vergleichen. Stimmen die beiden Prüfsummen überein, ist sichergestellt, dass das Paket während des Transports nicht modifiziert wurde. Ist dies nicht der Fall, wurde das Paket verändert.

Bei dem ESP-Protokoll funktioniert die Gewährleistung von Datenintegrität und Authentizität analog. Um mit dem ESP-Protokoll zusätzlich die Vertraulichkeit der Datenpakete sicherzustellen, wird abhängig vom verwendeten Betriebsmodus das komplette ursprüngliche IP-Paket (Tunnelmodus) oder nur die Nutzdaten (Transportmodus) verschlüsselt. Der dazu benötigte Schlüssel wurde ebenfalls zuvor mit dem IKE-Protokoll ausgetauscht.

5 Fazit

Die vorgestellten Techniken sind wichtige Werkzeuge um die Sicherheit in einem Netzwerk zu erhöhen. Allerdings genügt der Einsatz ausschließlich eines dieser Verfahren nicht, um den Schutz des Netzes zu gewährleisten. Erst das Zusammenspiel dieser Techniken steigert die Sicherheit des Netzes.

So macht zum Beispiel die alleinige Unterteilung eines Unternehmensnetzwerkes in mehrere Teilnetze mit Hilfe der VLAN-Technik wenig Sinn. Erst durch die zusätzliche Absicherung durch eine Firewall, sowohl ins Internet als auch zwischen den einzelnen Teilnetzen, erzielt man einen effektiven Schutz des Netzes.

Weiter sollte die Firewall, welche zwischen dem Internet und dem Intranet des Unternehmens eingesetzt wird, nicht nur aus einem einzigen Paketfilter bestehen. Auch hier stellt der Verbund aus mehreren Paketfiltern und einem Application-Level-Gateway einen hochwertigeren Schutz des Unternehmensnetzes dar. Die Einrichtung einer Demilitarized Zone in welcher die Paketfilter und das Application-Level-Gateway untergebracht sind, ist nochmal eine zusätzliche Steigerung der Sicherheit des Unternehmensnetzes.

Trotzdem existieren auch noch bei der Umsetzung der vorgestellten Maßnahmen zur Gewährleistung der Netzwerk-Sicherheit weitere Sicherheitslücken. So ist bei diesen Techniken der Faktor Mensch komplett ausgeblendet. Die Mitarbeiter eines Unternehmens können über mobile Speichermedien, wie zum Beispiel USB-Sticks, auf einfache Weise Daten in das geschützte Intranet importieren. Diese Daten werden nicht durch die Firewall kontrolliert und stellen ein hohes Risiko dar. Um dieses Risiko zu verringern, sind regelmäßige Sicherheitsschulungen im Umgang mit externen Daten der Mitarbeiter ein unverzichtbares Mittel.

6 Quellenverzeichnis

6.1 Literaturverzeichnis

[Q1] Kappes, Martin: Netzwerk und Datensicherheit. Wiesbaden 2007

[Q2] Pohlmann, Norbert; a Campo, Markus: Virtual Private Networks, Bonn 2001

[Q3] Pohlamm, Norbert: Firewall-System. Bonn 2001

[Q4] Dembowski, Klaus: Lokale Netze. München 2007

[Q5] Thomas Krenn http://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen [Stand: 28.11.2012]

[Q6] Spiegel-Online http://www.spiegel.de/netzwelt/gadgets/attacke-auf-playstation-netzwerk-hacker-stehlen-millionen-sony-kundendaten-a-759161.html [Stand: 30.11.2012]

6.2 Abbildungsverzeichnis

[A1] Kappes, Martin: Netzwerk und Datensicherheit. Wiesbaden 2007, Seite 159

[A2] Thomas Krenn http://www.thomas-krenn.com/de/wiki/VLAN_Grundlagen [Stand: 28.11.2012]