HANSER

VPN - Virtual Private Networks

Wolfgang Böhmer

Kommunikationssicherheit in VPN- und IP-Netzen, über GPRS und WLAN

ISBN 3-446-22930-2

Vorwort

Weitere Informationen oder Bestellungen unter http://www.hanser.de/3-446-22930-2 sowie im Buchhandel

Vorwort

Das Wort „virtuell“ *(lat. virtus, Tugend, Tapferkeit)* tauchte in den 50er Jahren zunächst als Begriff in der Computerwissenschaft auf. Virtuelle Computer spiegeln den Benutzern vor, dass sie allein Zugriff auf die Systemressourcen hätten, gleichwohl mehrere Benutzer sequentiell mit hoher Rechengeschwindigkeit an einem System arbeiten. Mittlerweile zu einem Modewort geworden, werden mit dem Ausdruck „virtuell“ Anpassungsfähigkeit und Interaktion, losgelöst von zeitlichen und örtlichen Beschränkungen, verknüpft. Sogar das Wort „virtuelle Unternehmen“ ist davon geprägt. Virtuelle Unternehmen zeichnen sich durch geschäftsorientierte zeitlich limitierte Partnerschaften aus, bei denen Lieferanten, Kunden und Produzenten aktiv und synergetisch einen Bedarf zum gemeinsamen Vorteil aller Beteiligten abdecken [Füser 1997].

Doch was ist unter „virtuell“ im Zeitalter der Informationsgesellschaft zu verstehen? Wie ist der Begriff des Nicht-Wirklichen, des Nicht-Realen, auf die Computerwelt bzw. auf das „Netz der Netze“ zu übertragen? Bei Scott et al. 1998 heißt es: „A virtual private network is a way to simulate a private network over a public network, such as the Internet“. Doch trifft diese Definition nicht den Kern. Besser ist es, ein Virtuelles Privates Netzwerk (VPN) allein durch logische Größen zu definieren und nicht durch physikalische. Die Grundidee ist, dass die Plattform, die physikalische Größe in erster Linie eine öffentliche Plattform sein muss. Dies können neben dem Internet auch andere Plattformen sein, wie z.B. die Sprachplattform Integrated Service Digital Network (ISDN), Weitverkehrsnetze (WAN) auf Basis eines Asynchronen Transfermodus (ATM) und Frame Relay (FR) oder auch Multi Protokol Label Switching (MPLS). Netzbetreiber (NSP) bieten ihren Kunden vielfach ein VPN auf dieser Basis an. Die Benutzung eines VPN wiederum kann man sich mit einer einfachen Metapher vorstellen: Das VPN-Gateway arbeitet wie ein Pförtner, der einen Verbindungskorridor zweier Gebäude bewacht und der nur jene Personen in den Korridor und damit in das andere Gebäude lässt die dazu berechtigt sind. Ein VPN ermöglicht einer bestimmten Anzahl von Teilnehmern einer öffentlichen Plattform, bei gleichzeitigem Ausschluss der Öffentlichkeit, miteinander zu kommunizieren resp. einen bestimmten Verbindungskorridor zu betreten. Eine anderes Analogon vergleicht ein VPN mit einem elektronisches Rohrpostsystem.

Dieses Buch gibt dem versierten Leser wie dem interessierten Laien einen umfassenden Einblick in die Technologie der VPN. Zunächst werden die Hintergründe und die Motivation zur Entwicklung der VPN-Technologie diskutiert. An zwei Beispielen wird die Spannbreite der unterschiedlichen Entwicklungsformen aufgezeigt. Dies wirft die Frage nach einer allgemeingültigen VPN-Definition auf; dieser ist ein eigener Abschnitt gewidmet. Anschließend werden die Netzwerk- und Kommunikationstechnologien für die VPN-Technologie diskutiert. Es werden die sieben Schichten des OSI-Referenzmodells vorgestellt, deren Kenntnis eine Unterscheidung zwischen einem Layer-2-VPN einem Layer-3- oder auch ei-

nem Layer-7-VPN erst ermöglicht.

Erläutert wird außerdem das Internetprotokoll IPv4 und die Version 6 (IPv6) sowie deren Unterschiede. Die Möglichkeiten des Internetprotokolls in Hinblick auf die Dienstgüten *(Quality of Service, QoS)*, die zwischen den Kommunikationspartnern realisierbar sind, werden ebenso betrachtet. Auch auf MPLS-VPN, als zukunftsweisende Technologie für ein VPN im Weitverkehrsnetz wird eingegangen. Da ein VPN häufig firmenübergreifend eingesetzt und mit einem Netzwerkanbieter realisiert wird, werden die Netztechnologien eines Weitverkehrsnetzes (WAN) diskutiert. Speziell die paketorientierten Vermittlungsverfahren, Frame Relay und ATM, welche auf Basis von Multiplexing-Verfahren arbeiten, werden skizziert. VPN auf dieser Basis werden als *trusted VPN* bezeichnet.

Secure VPN, die mittels Verschlüsselung gebildet werden, sind ein weiterer Bestandteil des Buches. Neben kryptographischen Verfahren nehmen die Themen Verschlüsselungsverfahren, Schlüsselmanagement und Schlüsselinfrastruktur einen breiten Raum ein. Im Sinne einer Zugriffsicherung werden sie zum Nachweis der Identität herangezogen. Außerdem werden sie eingesetzt, um die Integrität der Urheberschaft von elektronischen Dokumenten zu garantieren. Bei den Secuure VPN wird die Privatsphäre durch Nachrichtenverschlüsselung verwirklicht. Sie verhindert, dass unbefugte Dritte Nachrichten lesen oder manipulieren können.

Auf die unterschiedlichen Möglichkeiten verschiedener VPN-Varianten Intranet, Extranet- und Remote-Access-VPN wird anschließend eingegangen. Es wird ausführlich der bedeutsame Tunnelmechanismus und eine VPN-Realisierung auf verschiedenen OSI-Schichten erläutert. Der Quasi-VPN-Standard (IPSec) wird detailliert vorgestellt und es wird deutlich, wieviel Interoperabilitätsschwierigkeiten, trotz Spezifikationen der Internet Engineering Task Force (IETF), noch existieren.

Die sichere Kommunikation über fremde Netze, den Providernetzen, bildet einen weiteren Schwerpunkt des Buches. Seit kurzem existieren Referenzmodelle, auf die speziell eingegangen wird. Themen, wie z.B. Serviceleistungen eines Providers und deren Einhaltung, werden einer eigenen Betrachtung unterzogen. Abschließend wird die nicht triviale Planung eines VPN durch einen Vierphasenplan diskutiert.

Ziel des Buches ist es, die VPN-Technologie umfassend zu beschreiben. Kommentare, Anregungen oder auch Verbesserungsvorschläge sind jederzeit willkommen.

Frankfurt, im Frühjahr 2002

Wolfgang Böhmer
wjboehmer@t-online.de

Vorwort zur zweiten Auflage

Ich möchte an dieser Stelle den zahlreichen Rezensoren danken, die sich für den Hanser Verlag die Mühe gemacht haben, das Buch zu rezensieren und mir wertvolle Hinweise gegeben haben. Entstanden ist es zum großen Teil durch die Vorlesungen, die ich seit dem Sommersemester 2002 halte. Etliche Anregungen und Änderungswünsche, z.B. das Glossar und die Übungsaufgaben, die jetzt am Ende eines jeden Kapitels eingeflossen sind, rühren daher. Ebenso möchte ich den Studenten danken, die mir in den letzten Semstern durch zahlreiche Fragen und Diskussionen hilfreiche Anregungen und Verbesserungsvorschläge gaben.

Eine der gravierensden Änderungen ist durch die Neustrukturierung hervorgerufen worden. Es werden jetzt zuerst alle Grundlagen vermittelt und anschließend die VPN-Technologien secure VPN, trusted VPN und hybrid VPN diskutiert. Marktbetrachtungen und das Vierphasenmodell schließen das Buch ab. Die Definitionen der unterschiedlichen VPN-Technologien lehnen sich an den im Juli 2004 formulierten Vorschlag des inzwischen entstandenen VPN-Consortium an. Dies hat die Begriffe trusted VPN, secure VPN und hybrid VPN eingeführt. Im Abschnitt 1.3 des Kapitel 1 werden diese richtungsweisenden Begriffe detailliert erklärt.

Im Vergleich zur ersten Auflage wurden folgende Änderungen vorgenommen:

- Im Kapitel 1 wurde das zweite Beispiel durch ein Szenario aus dem Bereich Server Based Computing ersetzt. Damit wird der aufkommende mobile VPN-Bereich berücksichtigt.
- Im neu strukturierten Kapitel 2 wurden zahlreiche Ergänzungen und Korrekturen vorgenommen. Das Kapitel wurde aufgeteilt. Es vermittelt nun die notwendigen Grundlagen der VPN-Technologie. Die Diskussion der ATM, Frame Relay und MPLS Netze ist in das neu entstandene Kapitel 8 verschoben. Diese Art der VPN werden zukünftig als trusted VPN bezeichnet.
- Im Kapitel 3 wurden die Betrachtungen zur Unternehmensevaluierung erweitert und ergänzt. Einen Ausblick auf Reifegradmodelle wird außerdem gegeben.
- Im Kapitel 4 wurden die Ausführungen zur Hashfunktion überarbeitet. Ebenso wurde die Diskussion über AES – nachdem das Auswahlverfahren abgeschlossen ist – dem heutigen Sachstand angepasst.
- Im Kapitel 5 wurde das gegenüber RADIUS verbesserte Authentifizierungsverfahren DIAMETER aufgenommen.
- Das Kapitel 6 wurde gestrafft.
- Im Kapitel 7 werden die secure VPN diskutiert. Es werden u.a. ergänzende Betrachtungen zu IPSec aufgenommen. Die SSL-VPN sind nun stärker betont.

In diesem Kapitel sind die Betrachtungen zum WLAN und Mobilität in Verbindung mit der secure VPN-Technologie neu hinzugekommen.

- Das neu entstandene Kapitel 8 widmet sich den trusted VPN. Hier sind Teile vom Kapitel 2 eingeflossen.
- Im Kapitel 9 sind die Referenzmodelle überarbeitet und ausführlicher beschrieben.
- Im Kapitel 10 wurden die VPN-Marktbetrachtungen auf den aktuellen Stand gebracht. Ebenso wurden die Performance-Messungen überarbeitet und es wir ein überarbeiteter Vorschlag zur IPSec-Throughput-Messung vorgestellt.

Durch die zahlreichen Verbesserungen und zusätzlichen Erläuterungen, die in das Buch eingeflossen sind, ist die zweite Auflage substanziell verbessert worden. Doch ist das vorliegende Werk nicht als technische Anleitung zur Konfiguration (HowTo) von VPN zu verstehen. Zum einen gibt es für diesen Zweck bereits Literatur z.B. von [Spengenberg 2004], zum anderen ändern sich die technischen Implementierungen oftmals recht schnell.

Ihre Kritik, weitere Ideen und Verbesserungsvorschläge nehme ich gerne per E-Mail entgegen.

Darmstadt, im Mai 2005

Wolfgang Böhmer
wboehmer@cdc.informatik.tu-darmstadt.de