Diplomarbeit

Hochschule Mittweida (FH)
Fachbereich Mathematik / Physik / Informatik
Studiengang Informatik
Abgabe Mai 2005

Ronny Kämpfe

Analyse und Vergleich von VPN-Protokollen

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783956360466

Ronny Kämpfe

Analyse und Vergleich von VPN-Protokollen

Diplom.de

Ronny Kämpfe
Analyse und Vergleich von VPN-Protokollen

ISBN-10: 3-8324-9692-0
ISBN-13: 978-3-8324-9692-0
Druck Diplomica® GmbH, Hamburg, 2006
Zugl. Hochschule Mittweida (FH), Mittweida, Deutschland, Diplomarbeit, 2005

---

http://www.diplom.de, Hamburg 2006
Printed in Germany

Überblick:

Diese Diplomarbeit beschäftigt sich mit der Analyse und dem Vergleich ausgewählter am Markt erhältlicher VPN-Lösungen.

Zu Beginn wird die Motivation der Durchführung dieser Analyse durch SomSoft erläutert. Auf die Ziele und Anforderungen der Arbeit wird dabei eingegangen.

Kapitel zwei stellt die ausgewählten VPN-Lösungen vor und erklärt deren Funktionsweise und sicherheitsrelevante Aspekte. Dabei werden Schwachstellen aufgezeigt und erläutert und es wird auf die Interoperabilität zwischen verschiedenen Betriebssystemen oder Hardwareimplementierungen eingegangen.

Im dritten Kapitel wird die Installation, Konfiguration und Wartung der Lösungen erläutert. Von Interesse ist der Ablauf dieser Schritte sowie der Aufwand der Administration der VPNs.
Dabei werden mögliche Szenarien für VPNs aufgezeigt und die Implementierung dieser mit jeder der ausgewählten VPN-Lösungen getestet. Auf die notwendige Konfiguration wird dabei eingegangen sowie Probleme und Schwierigkeiten erfasst.

In Kapitel vier werden die Tests ausgewertet und die Vor- und Nachteile der Lösungen in verschiedenen Einsatzgebieten diskutiert.

Hinweis:

Inhaltsverzeichnis

1 Motivation und Ziele

1.1 Einleitung

SomSoft ist ein Unternehmen, welches in der Softwareentwicklung tätig ist. Die zu entwicklenden Projekte sind meist Datenbank-Anwendungen, welche in einer Client-Server-Struktur arbeiten wobei die Clients auch über das Internet mit dem Server kommunizieren. In einem aktuellen Projekt ist SomSoft an der Entwicklung eines Service-Management-Systems für die Automatisierungstechnik beteiligt, dessen Komponenten über eine recht komplexe Netzstruktur miteinander verbunden sind. Dabei werden vertrauliche Daten ausgetauscht, die momentan im Testbetrieb unverschlüsselt über das Netz und damit auch das Internet übertragen werden. Da dieser Umstand datenschutzrechtlich unzumutbar ist und von keinem Kunden, dank des gestiegenen Bewusstseins für die Sicherheit und Privatssphäre von Daten während des Transports im Internet, geduldet wird, sollen die Verbindungen per VPN geschützt werden. In anderen Projekten, die auch kleinere Unternehmen oder Privatleute betreffen, besteht ebenso der Wunsch nach Sicherheit bei der Dateübertragung.

1.2 Ziele

Ziel der Diplomarbeit ist es eine Übersicht der am Markt befindlichen Lösungen zur Implementierung von Virtuellen Privaten Netzwerken aufzustellen, ihre Funktionsweise zu analysieren und auf ihre Einsatztauglichkeit in verschiedenen Infrastrukturen zu testen. Im Mittelpunkt sollen dabei Sicherheitsaspekte wie verwendete Verschlüsselungsmethoden und Authentizitätssicherung stehen, aber auch Installation, Konfiguration und Wartung von mit den Lösungen zu implementierenden Netzen. Anhand der gewonnenen Erkenntnisse soll die Anwendbarkeit der Lösungen für Industrie und Wirtschaft sowie Privatanwender analysiert werden.

2 VPN-Technologien

„Ein virtuelles privates Netz (VPN) ist ein Netz von logischen Verbindungen zur Übermittlung von privaten Daten und Informationen bzw. Datenverkehr. Eine logische Verbindung ist eine Netzverbindung zwischen einem Sender und einem Empfänger, bei der der Weg der Informationen und die Bandbreite dynamisch zugewiesen wird.“[1, S.8]
VPNs sind Netzwerke, die zum Transport privater Daten meist öffentliche Netze wie bspw. das Internet nutzen. Die Verbindung wird dabei durch einen Tunnel zwischen VPN-Client und -Server realisiert, wobei dieser Tunnel oftmals durch Verschlüsselung geschützt wird. Auch ohne Verschlüsselung besteht bereits ein VPN, der eigentliche Schutz der Daten vor unbefugten Zugriffen wird dabei jedoch nicht gewährleistet. Da es am Markt zahlreiche VPN-Technologien gibt, welche unterschiedlicher Herkunft sind, verschiedene Ansätze verfolgen und unterschiedliche Einsatzgebiete bedienen können, sollen im Folgenden einige dieser Technologien vorgestellt werden. Dabei wird auf deren Funktionsweise eingegangen und die Umsetzung des Schutzes der transportierten Daten erläutert. Weiterhin werden Schwachstellen und die Interoperabilität zwischen verschiedenen Systemen aufgezeigt. Die untersuchten VPN-Lösungen sind:

- PPTP - Point-to-Point Tunneling Protocol
- IPSec
- L2TP - Layer 2 Tunneling Protocol
- Tinc - Tinc is not cabal
- OpenVPN

2.1 PPTP - Point-to-Point-Tunneling-Protokoll

2.1.1 Einleitung

Das Point-to-Point-Tunneling-Protocol [Zor99] stellt ein Protokoll dar, welches es erlaubt das Point-to-Point-Protocol über IP-Verbindungen zu tunneln. Es wurde in Zusammenarbeit mehrerer Firmen (u.a. Microsoft) entwickelt. Es ist dafür gedacht, Außendienstmitarbeitern (Roadwarrior) eines Unternehmens den Zugriff auf das Firmennetzwerk auf einfache Art und Weise zu ermöglichen. Microsofts Implementierung von PPTP ist stark in Verruf geraten, da deren Authentifizierungsmechanismen MS-Chap Version 1 und 2 große Sicherheitslücken aufweisen, wie von Schneier und Mudge [5] festgestellt wurde. Auf Microsofts Implementierung soll im folgenden genauer eingegangen werden, da diese in den meisten PPTP-Lösungen eingesetzt wird.

2.1.2 Funktionsweise

PPTP stellt eine Client-Server-Architektur dar, wobei der Server als PPTP-Network Server (PNS) und der Client, also das Endgerät, als PPTP-Access Concentrator (PAC) bezeichnet wird. Ein PPTP-Tunnel besteht aus zwei Verbindungen, einer TCP-Kontrollverbindung und einem IP Tunnel zur Datenübertragung, welche eine erweiterte Version des GRE-Protokolls [Net00] zur Tunnelung benutzt.

Die Kontrollverbindung

Zunächst wird eine TCP-Kontrollverbindung vom PAC oder PNS zum Port 1723/TCP der Gegenstelle aufgebaut. Dabei werden Zugangsinformationen, die Anzahl möglicher PPP-Verbindungen, die Fähigkeiten von PNS und PAC, sowie deren DNS-Namen übertragen. Diese Nachricht wird als Start-Control-Connection-Request (Start-CC-Request) bezeichnet und mittels Start-Control-Connection-Reply (Start-CC-Reply) beantwortet. Um die Bereitschaft von PAC und PNS auch ohne Übertragung von Nutzdaten zu überprüfen, wird im Intervall von 60 Sekunden ein Echo-Mechanismus ausgeführt, bei dem ein Echo-Request und als Antwort ein Echo-Reply gesendet werden. Bei Nichtbeantwortung eines Echo-Requests wird automatisch ein Stop-Control-Connection-Request gesendet, der zur Beendigung der Kontrollverbindung führt. Ist die Kontrollverbindung aufgebaut, werden über