FHTW

Fachhochschule
für Technik und Wirtschaft
Berlin
University of Applied Sciences

Netzwerk-Administration
Virtual Private Network mittels IPsec

Beleg

von

Mario Apitz
André Grüneberg
Janko Lötzsch

Version: 2.0 vom 15. Juli 2003

Inhaltsverzeichnis

Abbildungsverzeichnis **II**

1 Zielbestimmung **1**

2 Grundlagen **1**
2.1 Was ist ein VPN? . . . 1
2.2 Wozu dienen VPNs? . . . 1
2.2.1 Anwendungsbeispiel . . . 1

3 Verfahren **1**
3.1 OSI-Referenz-Modell . . . 1
3.2 Tunneln von PPP-Verbindungen über IP (Layer 2) . . . 2
3.2.1 Point-to-Point-Tunneling-Protokoll . . . 2
3.2.2 Layer-2-Forwarding . . . 2
3.2.3 Layer-2-Tunneling-Protocol . . . 2
3.3 Sicherheit im IP (Layer 3) - IPsec . . . 3
3.3.1 Der Transport-Modus . . . 3
3.3.2 Der Tunnel-Modus . . . 3
3.3.3 ESP – Encapsulating Security Payload . . . 4
3.3.4 AH – Authentication Header . . . 4
3.4 Exkurs – Kryptografische Verfahren . . . 5

4 Unser Fallbeispiel **5**

5 Zusammenfassung **6**

6 Quellen **6**

7 Anhang **9**

A XSR **9**

Abbildungsverzeichnis

1 OSI-Referenz-Modell 2
2 Paketaufbau in den IPsec-Modi 3
3 Aufbau eines ESP gesicherten Paketes 4
4 Aufbau eines AH gesicherten Paketes 4
5 Ausgangslage 7
6 kein VPN 7
7 VPN – zwischen den Fest-Standorten 8
8 VPN mit Road-Warrior 8

1 Zielbestimmung

Ziel ist es die Funktions- und Wirkungsweise eines Virtual Private Network (VPN) anhand der Protokoll-Lösung Internet Protocol SECurity (IPsec) anschaulich zu demonstrieren.

Auf die Verschlüsselung im Netzwerk und das Senden von vertraulichen Daten wie z.B. Passwörtern wird besonders eingegangen.

2 Grundlagen

2.1 Was ist ein VPN?

Der Zweck eines Virtual Private Networks ist der Aufbau eines Netzes von logischen Verbindungen zur Übermittlung von privaten Informationen bzw. Daten.

Eine logische Verbindung ist eine Netzverbindung zwischen Sender und Empfänger, bei der der Weg der Information und die Bandbreite dynamisch zugewiesen werden können.

2.2 Wozu dienen VPNs?

Die grundsätzliche Idee von Virtual Private Networks ist, die Vorteile einer offenen Kommunikations-Infrastruktur, wie dem Internet, zu nutzen. Gleichzeitig gilt es Authentizität, Integrität und Vertraulichkeit, die in unsicheren Trägermedien nicht gewährleistet werden können, sicherzustellen. Diesem Zweck dienen kryptografische Verfahren in den VPN-Protokollen.

2.2.1 Anwendungsbeispiel

Eine große Firma mit mehreren Standorten, unter anderem in Aachen und Berlin, hat früher mehrere tausend Euro im Jahr für Mietleitungen von der Deutschen Telekom AG bezahlt.

Heute setzt diese Firma auf VPN. Durch den Einsatz von VPN Gateways die nur noch eine Verbindung zum nächsten ISP[1] ihres geringsten Misstrauens benötigen, fallen die Kosten für die langsamen und teuren Mietleitungen weg.

Auch Außendienst-Mitarbeiter brauchen nur einen Zugang zum weltweiten Internet um mit ihrer Firma Daten und Information auszutauschen ohne auf die Sicherheit der Daten und Kommunikationspartner verzichten zu müssen.

3 Verfahren

3.1 OSI-Referenz-Modell

Die unterschiedlichen Protokolle, welche zum Einsatz kommen, werden im OSI Referenz Modell, wie in Abbildung 1 dargestellt, eingeordnet.

[1] ISP = Internet Service Provider

	OSI-Layer	TCP/IP-Layer	VPN
7	Applikation	Applikation (Anwendung)	
6	Präsentation		
5	Session		
4	Transport	Transport (Rechner)	
3	Netzwerk	Internet	IPsec
2	Datensicherung	Netzwerk (Netzzugang)	PPTP, L2F, L2TP
1	Physisch		

Abbildung 1: OSI-Referenz-Modell

3.2 Tunneln von PPP-Verbindungen über IP (Layer 2)

3.2.1 Point-to-Point-Tunneling-Protokoll

Das Point-to-Point-Tunneling-Protokoll (PPTP) geht auf eine Zusammenarbeit der Firmen Microsoft, 3Com, ECI Telematics, Ascend und US-Robotics zurück und basiert auf dem Point-to-Point-Protokoll (PPP). Es ist als Technologie relativ etabliert und wird üblicherweise im Endanwenderbereich eingesetzt, primär bedingt durch den Einfluss des Herstellers Microsoft, der PPTP in alle neueren Windows-Betriebssystemen einbaute. Eine enge Anbindung zu Windows NT ist durch die Authentifizierungs-Mechanismen PAP und CHAP sowie der für Windows-NT modifizierten Version MS-CHAP gegeben. In diesen Verfahren wurden in den letzten Jahren erhebliche Sicherheitslücken festgestellt. Bruce Schneier und Peter Mudge deckten schon 1999 diverse Schwachstellen in MS-CHAP auf, auf deren Grundlage bereits praktische Angriffe bekannt sind.

PPTP zielt darauf ab, den Fernzugriff für einzelne Anwender auf das Unternehmens-LAN über das Internet einfacher zu gestalten. Dies gelingt, indem die PPP-Frames um einen zusätzlichen Tunnel-IP-Header ergänzt werden. Der Rückgriff auf PPP erlaubt es, neben IP andere Protokolle wie IPX und NETBEUI zu übertragen. Damit steht PPTP einem breiten Anwendungsspektrum offen.

3.2.2 Layer-2-Forwarding

Das Layer-2-Forwarding (L2F) wurde von der Firma Cisco entwickelt und diente vornehmlich der Trennung zwischen Einwahl-Endgeräten und Zugangs-Routern. Es basiert, wie auch PPTP, auf PPP-Frames, die über IP transportiert werden.

3.2.3 Layer-2-Tunneling-Protocol

Um die beiden proprietären Verfahren PPTP und L2F unter einen Hut zu bringen und auch die Bedürfnisse anderer Hersteller zu berücksichtigen, wurde das Layer-2-Tunneling-Protocol (L2TP) entwickelt. Es vereint die Eigenschaften der beiden Ursprungs-Protokolle und definiert damit die künftige Entwicklung. Seine Verbreitung wird weiter zunehmen, da es Bestandteil von Windows 2000 und XP ist und somit weitflächig eingesetzt werden kann.

L2TP beinhaltet in der ursprünglichen Standardisierung keine Mechanismen zur Sicherheit. Dazu verweist der Standard auf die Möglichkeit IPsec (s.u.) einzusetzen. In Folge dessen haben sich aber einige proprietäre Erweiterungen um Sicherheits-Mechanismen etabliert.

3.3 Sicherheit im IP (Layer 3) - IPsec

IPsec – *Internet Protocol Security* ist eine sehr umfangreiche Protokoll-Suite und bietet zwei unterschiedliche Arbeits-Modi, den Transport- und Tunnel-Modus an. Sie unterscheiden sich durch den Aufbau der Paketergänzungen und durch ihre Einsatz-Möglichkeiten. Außerdem kann IPsec für jeden Modus die zwei verschiedenen Header ESP – *Encapsulating Security Payload* und AH – *Authentication Header* verwenden.

Des Weiteren umfasst die Suite ein Key Management namens Internet Key Exchange (IKE). Dieses dient dem zuverlässigen Austausch der kryptografischen Schlüssel zwischen den Kommunikations-Partnern.

Durch IPsec kann die Authentizität der Kommunikations-Partner, die Daten-Integrität und Daten-Vertraulichkeit sichergestellt werden.

IPsec bietet aber nur eine begrenzte Verkehrsfluss-Vertraulichkeit, da sowohl im Tunnel- als auch im Transport-Modus Protokoll-Header nicht verschlüsselt werden können. Anderenfalls wäre der Transport der Packete über ein IP-Netzwerk nicht möglich. IPsec schützt also nicht vor Veränderungen des Routing-Wegs und der Feststellbarkeit von vorhandenem Verkehr.

3.3.1 Der Transport-Modus

Im Transport-Modus verschlüsselt IPsec nur die Nutzlast des zu transportierenden IP-Paketes. Der Original-IP-Header bleibt erhalten und ein zusätzlicher IPsec-Header wird hinzugefügt (siehe Abbildung 2).

Vorteile ergeben sich durch den geringen Overhead und die ermöglichte Ende-zu-Ende-Sicherheit mit sehr feiner Granularität zwischen dem Absender und dem Empfänger des IP-Paketes.

3.3.2 Der Tunnel-Modus

Der Tunnel-Modus hat die zusätzliche Aufgabe, die Quell- und Ziel-Adresse auf dem Übertragungsweg explizit im öffentlichen Netzbereich oder im IP-Transit-Netz zu schützen (Abbildung 2).

Im Gegensatz zum Transport-Modus erhöht sich jedoch der Overhead des IPsec-Pakets durch den zusätzlichen IP-Header. Dies ermöglicht aber auch die für die End-Stationen transparente Verschlüsselung der Pakete. Da der Original-IP-Header im Tunnel-Modus verpackt wird, ist es für einen Mitlesenden nicht möglich, die ursprünglichen Absender und Empfänger festzustellen.

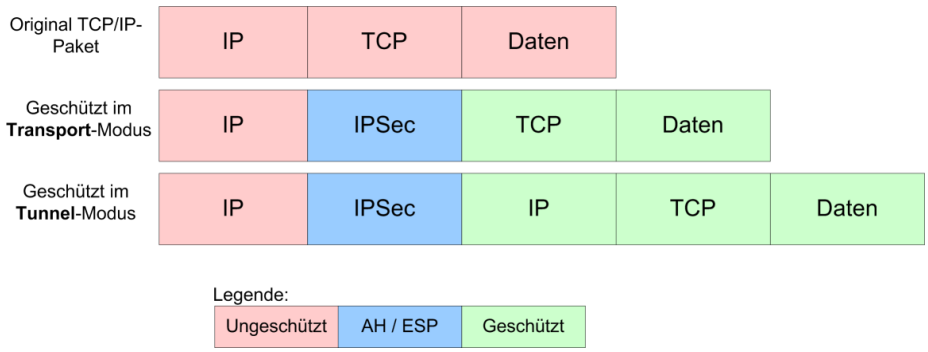

Abbildung 2: Paketaufbau in den IPsec-Modi

3.3.3 ESP – Encapsulating Security Payload

Das ESP-Protokoll dient der Verschlüsselung eines Datenpaketes und mittels Hash-Verfahren auch zur Integritäts-Sicherung der Daten (Abbildung 3). Zur Verschlüsselung können beliebige symmetrische Encryption-Verfahren (z.B. 3DES, AES) eingesetzt werden. Auch bei den eingesetzten Hash-Verfahren stehen verschiedene zur Wahl, u.A. MD5 und SHA1.

ESP sorgt für:

- Vertraulichkeit: Schutz vor unberechtigtem Mitlesen durch Verschlüsselung der Daten. Die Daten können nur von Personen gelesen werden, die den geheimen Schlüssel besitzen.
- Integrität: Der Originalzustand der Pakete kann durch Anwendung der Hash-Verfahren überprüft werden, dabei kann jede kleinste Änderung erkannt werden.
- Authentizität: Der Absender kann eindeutig festgestellt werden.

ESP benutzt eine symmetrischen Schlüssel, den beide Parteien zum Ver- und Entschlüsseln der Daten einsetzen. Das ESP-Protokoll kann sowohl im Transport-, als auch im Tunnel-Modus eingesetzt werden.

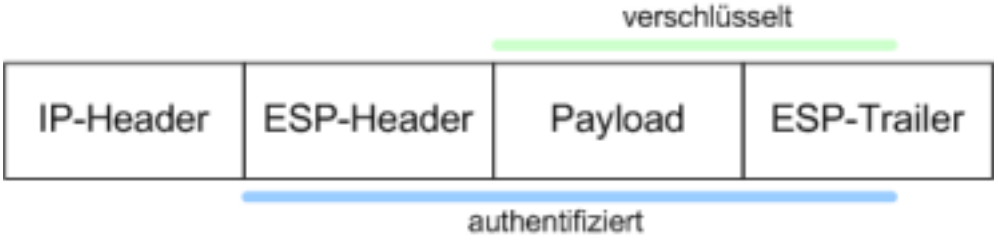

Abbildung 3: Aufbau eines ESP gesicherten Paketes

3.3.4 AH – Authentication Header

AH schützt Inhalte eines IP-Datagramms bis auf die veränderlichen Felder (mutable fields), die sich während des Transports verändern (Abbildung 4) und dient nur der Authentisierung. Die mutable fields werden bei der Berechnung als Null-wertige Felder angesehen. Der mit einer Hash-Funktion erhaltene Wert für Integritäts-Checks wird im AH mitgeführt.

AH sorgt für:

- Integrität: Checksumme wird generiert durch einen Hash-Verfahren (z.B. MD5 und SHA).
- Authentizität: Das Absender-Feld im IP-Header wird in die Überprüfung mit einbezogen.

Das AH-Protokoll kann sowohl im Transport-, als auch im Tunnel-Modus eingesetzt werden.

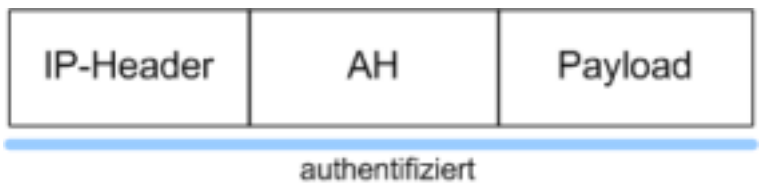

Abbildung 4: Aufbau eines AH gesicherten Paketes

3.4 Exkurs – Kryptografische Verfahren

Die vorgestellten VPN-Technologien haben sich die Sicherung der damit übertragenen Daten zum Ziel gesetzt. Um dieses Ziel zu erreichen, wird auf kryptografische Verfahren zurückgegriffen.

Dazu gehören symmetrische (zur Ver- und Entschlüsselung wird der selbe Schlüssel verwendet) und asymmetrische (es kommen Paare aus öffentlichem und geheimem Schlüssel zum Einsatz) Kryptografie- sowie Hash-Verfahren.

Bei symmetrischen Verfahren (z.B. DES, 3DES, AES) stehen die Kommunikations-Partner vor dem Aufbau einer gesicherten Verbindung vor dem Problem, dass Sie auf einem sicheren Wege den zu verwendenden Schlüssel austauschen müssen. Insbesondere bei großen Entfernungen, die VPNs überbrücken sollen, ist dies nicht immer leicht.

Daher bieten sich die asymmetrische Verfahren (auch als *Public-Key-Verfahren* bekannt) für die Kommunikation an. Dabei muss dem Sender nur der öffentliche Teil des generierten Schlüssel-Paars zur Verfügung gestellt werden, damit nur der Empfänger mit seinem privaten Schlüssel die gesendete Nachricht wieder entschlüsseln kann. Hier ist ist es natürlich notwendig, die Authentizität des Public-Keys sicherzustellen. Dies kann allerdings mit Hilfe eines vertrauenswürdigen Dritten (*trusted third party*) geschehen, der die Zusammengehörigkeit von Empfänger und seines Public-Key mit Hilfe einer digitalen Signatur beglaubigt.

Die asymmetrischen Kryptografie erfordert aber einen hohen Rechenaufwand, da dabei (z.B. im Falle von RSA) mit großen (Prim-)Zahlen umgegangen wird. Daher bedient man sich in der Praxis eines Hybrid-Verfahrens. Zu Beginn der Verbindung wird mit Hilfe von Public-Key-Verfahren ein Sitzungs-Schlüssel vereinbart, der im Folgenden für die eigentliche Kommunikation für die symmetrische Verschlüsselung eingesetzt wird.

Um die Daten-Integrität und -Authentizität zu gewährleisten kommen kryptografische Hash-Verfahren (z.B. MD5, SHA1) zum Einsatz. Diese bilden aus einem beliebig großen Datenblock einen Wert einheitlicher Länge, so dass kleinste Änderungen an den Daten bereits zu großen Änderungen des Hash-Wertes führen.

Da die Verfahren dieser Einweg-Funktionen bekannt sind, könnte jeder den zu einer Nachricht gehörigen Hash-Wert berechnen. Aus diesem Grund wird ein vereinbarter geheimer symmetrischer Schlüssel in die Berechnung des Wertes mit einbezogen – dieses Verfahren wird *Hashing Message Authentication Code* (HMAC) genannt. Der Empfänger kann dann unter Kenntnis des Schlüssels, der Nachricht und des verwendeten Algorithmusses das gleiche tun und das gewonnene Ergebnis mit dem übermittelten Wert vergleichen.

4 Unser Fallbeispiel

In unserem Fallbeispiel wollen wir den Bezug zur Praxis herstellen, deshalb können die eingesetzten Verfahren auch unter völlig anderen Bedingungen zum Einsatz kommen.

Eine mittelständische Firma mit mehreren Standorten in Deutschland einer in Aachen, München, Leipzig und Berlin hat von teuren Standleitungen auf eine VPN-Lösung umgerüstet. Des Weiteren beschäftigt die Firma mehrer Außendienst-Mitarbeiter, welche immer in einen der Filiale fahren mussten um Daten auf ihrem Notebook mit denen der Firma abzugleichen.

Die VPN-Lösung exemplarisch an den Standorten Aachen und Berlin, sowie einem Außendienst-Mitarbeiter (Road-Warrior) – erfordert in unserm Beispiel folgende Schritte:

- Kauf eines PCs, auf dem eine Linux Distribution installiert und FreeS/WAN[2] eingerichtet wird
- Kauf des VPN-Gateways XSR 1805 von Enterasys
- Kündigung der Miet-Leitung bei der Telekom
- Vertrags-Abschlüsse mit ortsansässigen ISPs

Ohne ein VPN, wie es in Abbildung 5 zu sehen ist, haben Angreifer aus dem Internet die Möglichkeit vertrauliche Daten, wie Passwörter, Loginnamen, zu empfangen oder sie sogar zu verändern.

In Abbildung 5 sind die zwei Standorte Berlin und Aachen – hier mit Standort A und B bezeichnet – ein Außendienst-Mitarbeiter und ein Angreifer – der Böse Bube – dargestellt. Dieser kann, wie in Abbildung 6 ersichtlich, sämtlichen Datenverkehr zwischen den Standorten mitschneiden (sniffen). Da er somit auch Logindaten mitlesen könnte, werden zwei VPN Gateways, eines an jedem Standort, eingerichtet (Abbildung 7).

Durch Einrichten eines VPNs zwischen den Standorten kann der *Böse Bube* zwar den VPN-Tunnel „von außen“ lesen, aber nicht dessen Inhalt.

Das Gleiche passiert, wenn der *Böse Bube* Daten unseres Road-Warriors mitlesen will. Die Notebooks der Außendienst-Mitarbeiter wurden ebenfalls mit einem VPN Client ausgerüstet (wir setzen SSH Sentinel ein) und haben damit die Möglichkeit sich von jedem beliebigen Punkt aus dem Internet im Firmen-VPN anzumelden (Abbildung 8).

Die Firma braucht sich ab sofort keine Sorgen mehr zu machen, wenn sie ihre Daten durch das Internet sendet. Die Außendienst-Mitarbeiter brauchen nur eine Internetanschluss (z.B. Internet-Cafe) und müssen nicht eine der Filialen anfahren.

5 Zusammenfassung

Mit der Errichtung eines VPNs haben wir gezeigt, dass einem Außenstehenden nicht mehr die Gelegenheit gegeben wird Daten mitzulesen.

6 Quellen

- RFC 2401 IPsec Architektur
- RFC 2402 IP Authentication Header (AH)
- RFC 2403 AH mit MD5-96
- RFC 2404 AH mit SHA-1-96
- RFC 2405 ESP mit DES-CBC
- RFC 2406 Encapsulation Security Payload (ESP)
- RFC 2408 ISAKMP

[2]FreeS/WAN ist eine Linux Implementation des IPsec Protokolls

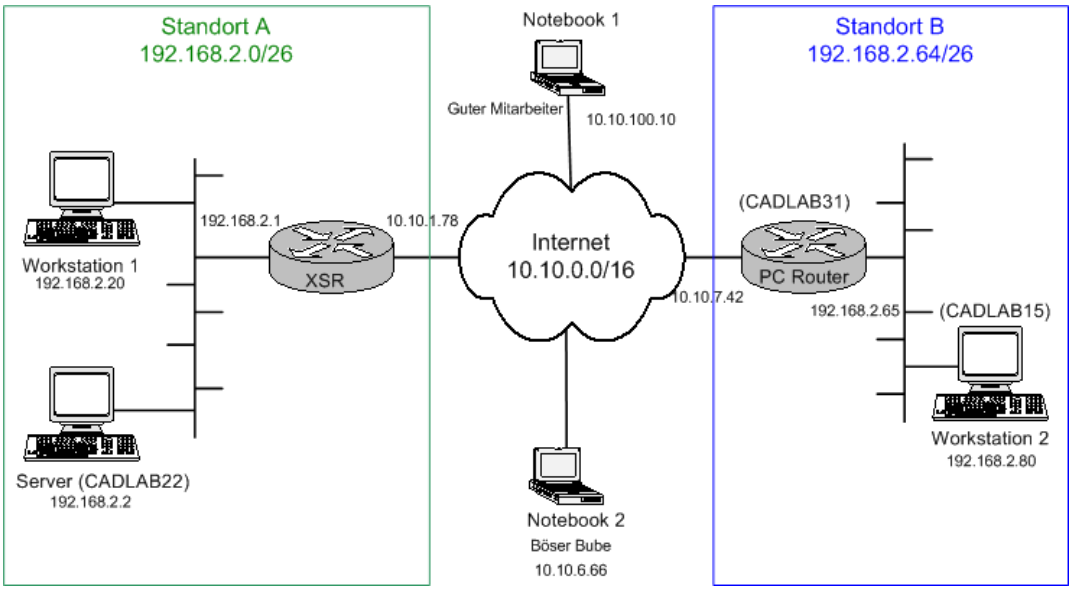

Abbildung 5: Ausgangslage

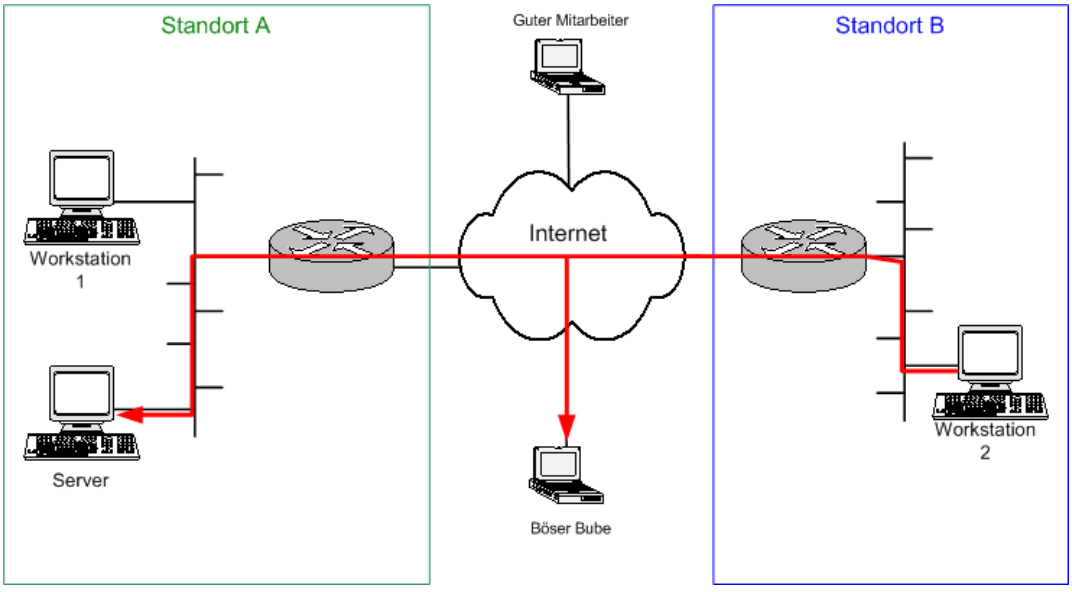

Abbildung 6: kein VPN

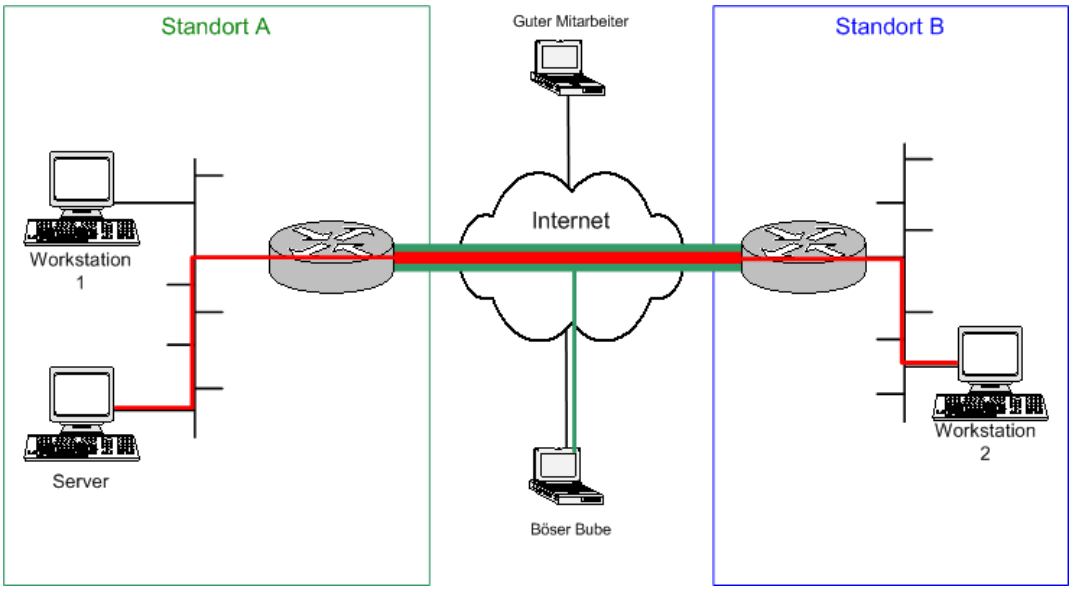

Abbildung 7: VPN – zwischen den Fest-Standorten

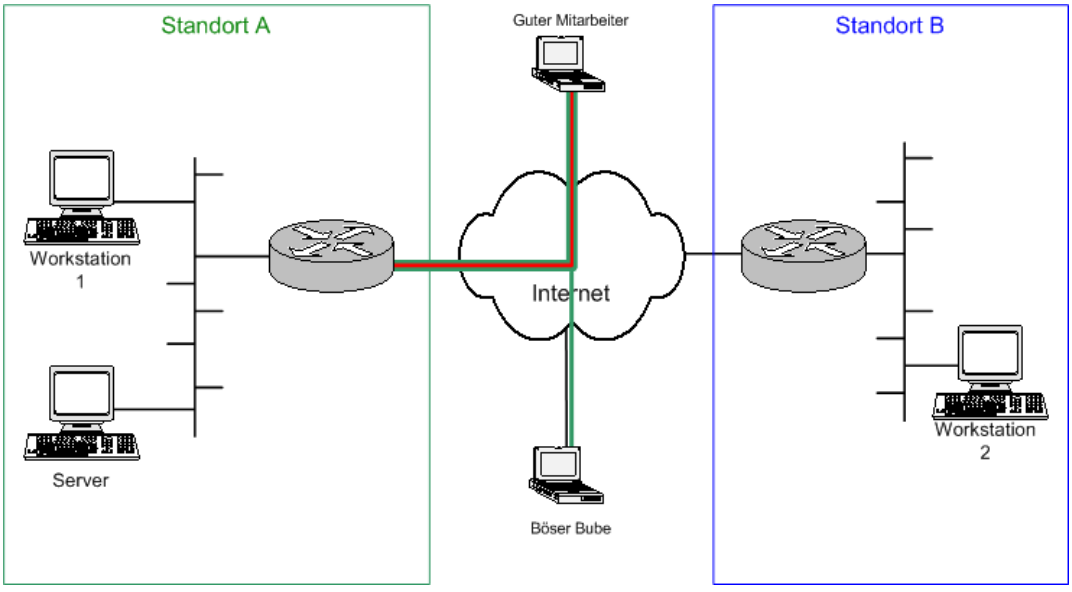

Abbildung 8: VPN mit Road-Warrior

- RFC 2409 Internet Key Exchange (IKE)
- Wolfgang Böhmer:*Virtual Private Networks, 2002*
- *Bruce Schneier:*Angewandte Kryptographie, 1996
- http://www.freeswan.org
- http://www.enterasys.com

7 Anhang

A XSR

Der XSR-1805 ist ein IP-Router mit WAN[3]- und VPN-Unterstützung. Des weiteren werden L2TP, IPsec, PPTP, sowie die verschiedenen Authentifikations-Protokolle, mit 3DES- und AES-Verschlüsselung angeboten. Zusätzlich beinhaltet der XSR einen Packet-Filter für den Einsatz in Firewalls sowie Dragon IDS[4].

Vom Enterasys Operating System (EOS) werden folgende Funktionalitäten unterstützt: die Routing-Protokolle Routing Information Protocol (RIP) und Open Shortest Path First (OSPF), DHCP[5]-Server, ISDN[6] und Frame Relay.

[3]Wide Area Network
[4]Intrusion Detection System
[5]Dynamic Host Configuration Protocol
[6]Integrated Services Digital Network