Integration eines VPN-Dienstes auf Basis von Transport-Layer-Verschlüsselung

Erweiterung eines Intranets zur Bereitstellung einer Fernzugriffsmöglichkeit

Betriebliche Projektarbeit
für die Abschlussprüfung im Sommer 2007

zum Fachinformatiker der Fachrichtung Systemintegration

Projektdokumentation vorgelegt von:
Volker Böcker
(Prüflingsnr. 7395)

Projektzeitraum:
1. bis 18. April 2007

Ausbildungsbetrieb

Deutsche Telekom AG
Telekom Training
Berufsausbildung Bremen
Utbremer Str. 90
28217 Bremen

Prüfungsbetrieb

T- Systems Enterprise Services GmbH
Service Line Systems Integration
ICT- Service
Utbremer Str. 90
28217 Bremen

Durchführung der Abschlussprüfung

Handelskammer Bremen
Am Markt 13
28195 Bremen

Prüfungsteilnehmer

Volker Böcker
Hemmstr. 278
28215 Bremen

Inhaltsverzeichnis

1. Einleitung 1
1.1 Motivation und Projektauswahl 1
1.2 Vorstellung des Kunden 1
1.3 Änderungen zum Projektantrag 1
1.4 Projektablauf und Ansprechpartner 2

2. Analyse und Planung 2
2.1 Vorhandene Infrastruktur und Dienste 2
2.2 Anforderungen des Kunden 3
2.3 Das angebotene Konzept und der Soll-Zustand 4
2.4 Aufstellung der durchzuführenden Arbeiten 5
2.5 Abgrenzung alternativer Umsetzungsmöglichkeiten 6
2.6 Begründung der getroffenen Entscheidungen 6

3. Kalkulation und Beschaffung 7
3.1 Aufstellung der benötigten Komponenten 7
3.2 Auswahlkriterien und Angebote 7
3.3 Die notwendigen Internetanbindungen 9
3.4 Kostenkalkulation in tabellarischer Übersicht 9

4. Installation und Konfiguration 10
4.1 Installation Phase I – Durchführung im eigenen Betrieb 10
4.1.1 Betriebssystem-Installation des VPN-Servers 10
4.1.2 Installation der VPN-Anwendung 11
4.1.3 Das Installationspaket für die Systemadministratorin 13
4.2 Installation Phase II – Vor-Ort-Installation beim Kunden 13
4.2.1 Aufstellen und Inbetriebnahme des Servers 13
4.2.2 IP-Konfiguration des Intranets 13
4.2.3 Einrichten des VPN-Clients 14
4.2.4 Funktionstest 15

5. Projektabschluss 15
5.1 Datensicherung der erstellten Konfiguration 15
5.2 Übergabe des Systems an den Kunden 15
5.3 Schlussbemerkungen 16

6. Anhang 17
6.1 Netzwerkplan Baumann Immobilien 17
6.2 Angebote für die Server-Hardware 18
6.2.1 Angebot Gebrauchtware, eBay-Händler 18
6.2.1 Angebot Neuware, ALTERNATE GmbH, Onlineshop 23
6.3 Konfigurationsdateien 24
6.3.1 Konfigurationsdatei des OpenVPN-Servers 24
6.3.2 Konfigurationsdatei des OpenVPN-Clients 25

1. Einleitung

1.1 Motivation und Projektauswahl

Die hier vorgelegte betriebliche Projektarbeit zur Absolvierung der Abschlussprüfung zum Fachinformatiker für Systemintegration umfasst die Planung und Integration eines virtuellen privaten Netzwerkes (VPN) auf Basis des Transport Layer Security-Protokolls (TLS). Kernaufgabe des Projektes ist die Erweiterung eines bestehenden Intranets zur Bereitstellung einer verschlüsselten Zugriffsmöglichkeit von außen.

Mit der stetig fortschreitenden Integration netzgestützter Dienste in den Arbeitsalltag entwickelt sich ein steigender Bedarf an einer ortsunabhängigen Verfügbarkeit der integrierten Dienste und Applikationen. Diese Entwicklung lässt sich nahezu überall dort beobachten, wo Informationstechnik eingesetzt wird – eine Beschränkung auf die klassische Situation eines Außendienstmitarbeiters im Großkundenumfeld würde dem Stand der Dinge längst nicht mehr gerecht. Damit existiert ein großes Potential zur Integration von VPN-Diensten in vielen unterschiedlichen Zielgruppen.

Als Auszubildender der Deutschen Telekom AG arbeite ich seit Januar 2005 bei der T-Systems Enterprise Services GmbH in der Abteilung Information and Communication Technology Service (ICTS) – diese Abteilung betreibt für ca. 500 Software-Entwickler und Mitarbeiter an den Standorten Bremen und Hamburg ein geschlossenes Netz mit Anbindung an das Telekom-Intranet und einer eigenen DMZ zur Bereitstellung von Diensten im Internet. Kernaufgabe der 14 ICTS-Kollegen ist das Netzwerk-Management, die Bereitstellung von TK-Anschlüssen sowie Betrieb und Wartung von ca. 600 Arbeitsplatz-Rechnern und 200 Servern.

Im Rahmen dieser Abteilung legte ich nach dem Kennenlernen der verschiedenen Tätigkeitsbereiche meinen persönlichen Schwerpunkt auf den Bereich Firewall-Administration und VPN-Konfiguration. Da es sich betriebsbedingt hierbei jeweils um ausgereifte Enterprise-Lösungen handelt, möchte ich die erlernten Kompetenzen für das Abschlussprojekt auf eine andere Zielgruppe übertragen, und zwar den Bereich der Kleinbetriebe.

1.2 Vorstellung des Kunden

Da die ICTS in ihrer derzeitigen Funktion nicht für externe Auftraggeber agiert, wird zur vollständigen Durchführung des Projektes der fiktive Auftragnehmer Bocom GmbH verwendet, ein in Bremen ansässiges IT-Systemhaus mit 6 Angestellten.

Auftraggeber ist ein Bauträger- und Hausverwaltungsbüro mit einem Geschäftsführer und 5 Angestellten. Der Kunde repräsentiert einen typischen Kleinbetrieb, so dass hinsichtlich der finanziellen und technischen Dimensionierung ausdrücklich keine Enterprise-Lösungen zum Einsatz gebracht werden können. Aus datenschutzrechtlichen Gründen wird der Name des real existierenden Kunden für die Dokumentation in Baumann Immobilien geändert.

1.3 Änderungen zum Projektantrag

Bei der Durchführung des Projektes ergaben sich hinsichtlich des Projektablaufs und damit auch bezüglich der ursprünglich kalkulierten Arbeitszeiten einige Änderungen. Im Gegensatz zur ursprünglichen Planung erforderte die Besprechung mit dem Kunden und die Erstellung des Gesamtkonzeptes mehr Zeitaufwand als geplant. Da es sich um zwei entscheidende Aspekte für die erfolgreiche Durchführung des Projektes handelt, wurde die erforderliche Umstrukturierung des Projektablaufes bewusst in Kauf genommen. Die vormals geplante Erstellung von je einem Merkblatt für die Anwender und die Administration wurde aus dem Projektplan gestrichen. Die

notwendigen Informationen für den Kunden werden nun in dem Übergabegespräch kommuniziert. Außerdem wurde für die Erstellung der Projektdokumentation eine zusätzliche Arbeitsstunde veranschlagt.

1.4 Projektablauf und Ansprechpartner

Das Projekt wird in drei Abschnitte unterteilt. Im ersten Abschnitt, der Planungsphase, wird der Ist-Zustand vor Ort geprüft und in einem ausführlichen Gespräch mit dem Kunden Leistungsumfang und Konditionen des Projektauftrages besprochen. Anschließend erfolgt im zweiten Abschnitt die Beschaffung der benötigten Komponenten sowie die Installation des Servers und die Vorbereitung aller weiteren benötigten Bestandteile, wie der Konfigurationspakete für die Clients und die Erstellung des IP-Adress-Konzeptes. Dieser Projektabschnitt wird im eigenen Betrieb und nicht beim Kunden durchgeführt. Damit ergeben sich folgende Vorteile:

- Möglichkeit eines ausführlichen Tests des Servers
- Vor-Ort-Installation beim Kunden kann sorgfältig vorbereitet werden
- die Ausfallzeit des Kunden-Intranets kann möglichst gering gehalten werden

Der dritte Projektabschnitt umfasst die eigentliche Integration des vorinstallierten Systems beim Kunden, den abschließenden Funktionstest und die Übergabe. In Absprache mit dem Geschäftsführer wird dies an einem Samstag außerhalb der regulären Bürozeiten durchgeführt.

Der Ansprechpartner auf Seite des Kunden ist der Geschäftsführer Herr Baumann. Mit ihm werden alle Sachverhalte besprochen und der Gesamtauftrag ausgehandelt. Für sämtlichen Schriftverkehr und die Regelung des Zutritts für die Vor-Ort-Installation verweist Herr Baumann auf die Buchhalterin Frau Baumann. Was den Zugang zu den vorhandenen Systemen des Intranets und andere technische Details betrifft, so dient die Systemadministratorin der Baumann Immobilien, Frau Mohn, als Schnittstelle für das Projekt.

Auf betrieblicher Seite dient Herr Pachowsky von der Abteilung ICTS als Ansprechpartner zur Durchführung des Projektes. Sämtliche Fragen und mögliche Probleme hinsichtlich des Projektablaufs können mit Herrn Pachowsky geklärt werden.

2. Analyse und Planung

Für den ersten Projektabschnitt findet eine Besprechung mit dem Geschäftsführer Herrn Baumann in seinen Büroräumen statt. Hierbei wird zunächst der status quo erörtert. Für technische Fragen und Auskünfte nimmt die Systemadministratorin Frau Mohn telefonisch an dem Gespräch teil. Im Folgenden wird der Ist-Zustand dokumentiert.

2.1 Vorhandene Infrastruktur und Dienste

Vorhanden ist eine Microsoft Windows-Domäne mit einem Domänen-Controller, fünf Arbeitsplatz-Rechnern und einem Notebook. Folgende Anwendungen kommen zur Bewältigung des Tagesgeschäftes zum Einsatz:

- Microsoft Office für Textverarbeitung und Tabellenkalkulation
- Microsoft Outlook für E-Mail-Dienste, Termin-, Kontakt- und Aufgabenverwaltung
- PublicShareFolder (DCOM-basierte Groupware-Lösung für Microsoft Outlook)
- DOMUS-Hausverwaltungssoftware

- ProfiCash als HBCI-Onlinebanking-Programm
- zentraler Fileserver über SMB
- zentraler Printserver für zwei Laserdrucker

Es existiert ein 100 Mbps Ethernet mit sternförmiger CAT5-Twisted-Pair-Verkabelung. Der vorhandene Server sowie alle Netzkomponenten befinden sich in einem Kellerraum im Untergeschoss des Bürogebäudes. Für die Internetanbindung kommt eine AVM FRITZ!Box SL zum Einsatz, die gleichzeitig als DHCP- und DNS-Server fungiert und für die Nutzung des T-DSL Business-Anschlusses die erforderliche Network Adress Translation (NAT) realisiert.

Administriert wird das Netzwerk von einer Teilzeitkraft auf Stundenbasis, die für Wartungsarbeiten jeweils an Wochenenden vor Ort ist und akute Störungen durch zeitaufwändige telefonische Anleitung der Angestellten beheben muss. Durch die begrenzte Anwesenheitszeit an den Wochenenden können reguläre Wartungsarbeiten oft nicht oder nur sehr verzögert geleistet werden, da die angesammelten Störungen bevorzugt abgearbeitet werden müssen.

Es kommt häufig vor, dass der Geschäftsführer oder die Sachbearbeiter der Hausverwaltung außerhalb der regulären Geschäftszeiten auf die gemeinsamen Terminkalender und Kontakte-Ordner zugreifen müssen. Auch die Buchhalterin benötigt regelmäßig außerhalb der Bürozeiten bestimmte Informationen aus der Onlinebanking-Software. Dies ist auch darin begründet, dass es sich bei der Baumann Immobilien um einen typischen selbstständigen Familienbetrieb handelt.

Da es derzeit ausschließlich die Möglichkeit gibt, direkt von den Büro-Arbeitsplätzen aus auf den Server und die Daten zuzugreifen, entstehen allen Beteiligten erheblicher Aufwand und Kosten durch außerordentliche Anfahrten, die zudem Organisation und Zeit erfordern. Zudem erschwert und verzögert diese Situation sowohl die Beantwortung von Kundenanfragen als auch die Reaktion auf Störungen oder Notfälle bei den durch die Baumann Immobilien verwalteten 600 Mietwohnungen.

2.2 Anforderungen des Kunden

Im weiteren Verlauf der Besprechung mit Herrn Baumann und Frau Mohn äußert der Geschäftsführer seine Wünsche und Anforderungen an die mögliche Investition in eine VPN-Lösung. So werden im Folgenden die Anforderungen aus Anwendersicht festgehalten.

Der Kunde möchte die Möglichkeit haben, von seinem Heimarbeitsplatz aus auf das Büro-Netzwerk zuzugreifen, um den gemeinsamen Datenspeicher nutzen und eine Anbindung an das zentrale Outlook herstellen zu können. Außerdem ist es entscheidend, von dem Heimarbeitsplatz aus die eingesetzte Onlinebanking-Software benutzen zu können, auch hierfür ist eine Verbindung zum zentralen Server notwendig.

Der zweite wichtige Aspekt für die Einrichtung einer Fernzugriffsmöglichkeit besteht in dem Wunsch des Kunden, der Netzwerkadministratorin einen Wartungszugang zur Verfügung zu stellen. Damit bietet sich Frau Mohn die Möglichkeit, einen Großteil der anfallenden Wartungsarbeiten sowie akute Entstörungen zeitnah und effizient durchzuführen, da sie nicht mehr zwangsläufig vor Ort sein muss.

Eine Zugriffsmöglichkeit für die beiden Sachbearbeiterinnen der Hausverwaltung soll vorerst noch nicht eingerichtet werden, da Herr Baumann in einer Testphase zunächst selbst bewerten möchte, inwieweit sich die Nutzung eines VPN-Zugangs im Geschäftsalltag etabliert.

Da auf dem zentralen Server sensible Geschäftsdaten abgelegt sind, ist es für Herrn Baumann eine zwingende Voraussetzung, dass bei der Integration einer Zugriffsmöglichkeit von außen der Aspekt der sicheren Authentisierung gewährleistet ist.

2.3 Das angebotene Konzept und der Soll-Zustand

Im Namen der Bocom GmbH wird für die Baumann Immobilien folgendes Konzept erstellt:

[1] Die Umsetzung des VPN-Zugangspunktes für das Intranet erfolgt durch einen dedizierten Server, der dafür beschafft wird. Als Betriebsystem wird der Ubuntu 6.06.1 LTS Server verwendet, der auf Debian Linux basiert.

[2] Als Software kommt OpenVPN in der Version 2.0.9 zum Einsatz, das zur Verschlüsselung des VPN-Tunnels das Transport Layer Security-Protokoll (TLS) verwendet. Es wird ein Site-to-End VPN eingerichtet, so dass sich mehrere Clients zeitgleich an dem Server anmelden können (Site-to-End = Punkt [Server] zu Mehrpunkt [Clients])

[3] Die Authentifizierung erfolgt mittels selbst signierter X.509-Zertifikate, die für den Server und jeden Client erstellt werden. Die Zertifizierungsstelle wird ebenfalls auf dem Server eingerichtet und mittels der in OpenVPN integrierten OpenSSL-Suite realisiert.

[4] Es wird der so genannte Tunnelmodus konfiguriert. Damit arbeitet das VPN auf Schicht 3 des OSI-Referenzmodells, so dass der Server ein eigenes IP-Subnetz für die Clients zur Verfügung stellt. Dafür müssen entsprechende Routingfunktionen eingerichtet werden.

[5] Das gesamte Intranet wird über das VPN erreichbar sein, es werden keine individuellen Zugriffsbeschränkungen eingerichtet.

[6] Der Server muss über einen Port aus dem Internet erreichbar sein, dieser muss durch den DSL-Router weitergeleitet werden. Da der Kunde keine eigene feste öffentliche IP-Adresse besitzt, muss die Erreichbarkeit von außen über einen festen Namen mittels eines Dienstanbieters für dynamisches DNS erfolgen.

[7] Sowohl am Standort des Servers als auch am Heimarbeitsplatz werden die vorhandenen Internetanbindungen hinsichtlich der Bandbreite geprüft und ggf. aufgerüstet.

[8] Auf dem vorhandenen Windows NT Domänen-Controller wird ein WINS-Serverdienst eingerichtet, um die Namensauflösung zentral verfügbar zu machen.

[9] Es werden zwei VPN-Clients eingerichtet und zwar der Heimarbeitsplatz-PC des Geschäftsführers und das vorhandene Notebook für den Einsatz unterwegs. Die Clients werden netzwerktechnisch angebunden, die Konfiguration der betreffenden Anwendungsprogramme erfolgt durch die Systemadministratorin.

[10] Für den Fernzugriff der Administratorin wird ein Installationspaket mit Kurzanleitung erstellt.

[11] Nach Abschluss der Installation wird einmalig eine Datensicherung der OpenVPN-Konfiguration angefertigt.

[12] Der Kunde wird bei Übergabe des Systems über die technischen Limitierungen des VPNs informiert.

Anmerkungen zum angebotenen Konzept

In Absprache mit Herrn Baumann erfolgt die Integration der neuen Funktionalitäten derart, dass für den Anwender kein zusätzlicher Bedienungsaufwand entsteht, die Einbindung erfolgt quasi transparent. Dazu wird die OpenVPN-Anwendung sowohl server- als auch clientseitig als Systemdienst eingebunden. Damit steht die VPN-Verbindung nach dem Hochfahren der Rechner automatisch zur Verfügung.

Nach Abschluss des Projektes steht ein Einwahlpunkt in das Intranet der Baumann Immobilien zur Verfügung, über den sämtliche Dienste genutzt werden können, die auf dem IP-Protokoll aufbauen.

Durch eine Eigenschaft des OpenVPN-Netzwerktreibers im Tunnel-Modus ergibt sich die Einschränkung, dass in dem VPN-Subnetz IP-Broadcastpakete nicht ordnungsgemäß empfangen werden können. Solche Dienste, die diese Funktionalität benötigen, sind damit also nicht verwendbar.

Dies stellt jedoch für die praktische Nutzung des VPNs bei der Baumann Immobilien keinen Nachteil dar. Durch die genannte Einschränkung funktioniert zwar die Broadcast basierte Namensauflösung von Windows zum Durchsuchen der Netzwerkumgebung und Ansprechen von Rechnern über Kurznamen nicht – dieses Problem lässt sich aber folgendermaßen vollständig lösen. Auf dem vorhandenen Domänen-Controller wird zusätzlich ein WINS-Serverdienst installiert, über den dann die Namensauflösung mittels dynamischer Registrierungen der Computernamen (Kurznamen) und Dienste erfolgt. Dieser erforderliche Dienst lässt sich auf dem vorhandenen Microsoft Windows NT 4.0 Server problemlos integrieren, da das Betriebssystem die entsprechenden Funktionalitäten bereits mitbringt.

OpenVPN bietet die Möglichkeit, den VPN-Clients beim Verbindungsaufbau nicht nur statische Routen für die Erreichbarkeit serverseitiger Subnetze, sondern auch IP-Adressen von DNS- und WINS-Servern zu übermitteln. Auf den Clients des Intranets kann der zu verwendende WINS-Server in der Netzwerkkonfiguration eingetragen werden.

Damit ist eine Auflösung von aus dem Intranet bekannten Kurznamen auch für per VPN verbundene Rechner direkt verfügbar.

2.4 Aufstellung der durchzuführenden Arbeiten

Nr.	Tätigkeit	Arbeitszeit
A. Vorbereitung		
01	Sichten der vorhandenen Infrastruktur und Dienste	1,0 Std.
02	Besprechung mit dem Kunden (Planung, Anforderungen)	2,0 Std.
03	Abgrenzen alternativer Umsetzungsmöglichkeiten	1,0 Std.
04	Erstellen des Konzeptes	2,5 Std.
05	Einholen von Angeboten für die benötigte Hardware	1,0 Std.
B. Installation Phase I – Durchführung im eigenen Betrieb		
06	Installation und Grundkonfiguration des Server-Betriebssystems	3,5 Std.
07	Installation von OpenVPN und der benötigten Zusatzpakete	1,0 Std.
08	Erstellung der Public Key Infrastruktur (PKI)	2,0 Std.
09	Erstellung der Konfigurationsdateien für den VPN-Tunnel	2,0 Std.
C: Installation Phase II – Vor-Ort-Installation beim Kunden)		
10	Aufstellen und Inbetriebnahme des Servers	1,0 Std.
11	Anpassung des Intranets (statische Adressen, Routing)	2,0 Std.
12	Installation von OpenVPN auf dem Notebook	1,0 Std.
13	Installation von OpenVPN auf dem Heimarbeitsplatz-PC	1,0 Std.
14	Funktionstest des Gesamtsystems	2,0 Std.
D. Projektabschluss		
15	Anfertigung einer Datensicherung	1,0 Std.
16	Einweisung des Kunden und Übergabegespräch	2,0 Std.
E. Erstellung der Projektdokumentation		9,0 Std.
Gesamtarbeitszeit		35,0 Std.

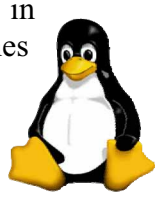
2.5 Abgrenzung alternativer Umsetzungsmöglichkeiten

Für die Implementierung eines virtuellen privaten Netzwerkes existieren zahlreiche Möglichkeiten. Diese unterscheiden sich nicht nur hinsichtlich der Dimensionierbarkeit, sondern insbesondere auch durch die verwendeten Protokolle, die Verschlüsselungsalgorithmen und die zur Integration verwendete Schicht des OSI-Referenzmodells. Auch bezüglich der eingesetzten Authentisierungs- und Authentifizierungs-Modelle gibt es viele Variationen. Beispielhaft seien im Folgenden drei alternative Umsetzungsmöglichkeiten aufgezeigt.

- Die Betriebssysteme der Microsoft-Produktfamilie des Windows 2003 Servers bieten – mit Einschränkungen bei der Version „Web-Edition“ – einen umfangreichen Funktionsumfang für ein VPN-Gateway. Die Anzahl der gleichzeitig verfügbaren Client-Verbindungen wird hier in erster Linie durch die Leistung der verwendeten Server-Hardware bestimmt.
- Im Bereich der Hardware-Router für xDSL- und Kabelnetz-Internetzugänge implementieren Hersteller wie z. B. Draytek mit den höheren Modellen der Router-Serie „Vigor“ VPN-Funktionalitäten. Da es sich um dedizierte Hardware-Appliances handelt, ist die Anzahl der möglichen Clients fest vorgegeben und zur Verbindungs-Herstellung wird häufig eine proprietäre Software verwendet.
- Kommerzielle Internet-Service-Provider bieten vermehrt webbasierte VPN-Dienste an. Beispielsweise führt die Festnetz- und Breitbandsparte der Deutschen Telekom AG T-Com im Rahmen des Internetdienstes T-Online das Produkt „directVPN“. Der gewählte Tarif entscheidet über den Leistungsumfang der VPN-Funktionen. Derartige Services stellen für den Anwender eine vollständig ausgelagerte Lösung dar.

2.6 Begründung der getroffenen Entscheidungen

Die Wahl von OpenVPN auf Basis eines separaten Linux-Servers bietet aus Sicht der Bocom GmbH entscheidende Vorteile gegenüber anderen Umsetzungsmöglichkeiten. Mit dem gewählten System wurden in der Vergangenheit bei verschiedenen Kunden und in unterschiedlichen Umgebungen bereits viele positive Erfahrungen hinsichtlich eines stabilen Betriebs und einer guten Administrierbarkeit gemacht.



Das Konzept von OpenVPN bietet eine gute Skalierbarkeit und sowohl client- als auch serverseitig sind die Netzwerk- und Systemanforderungen verhältnismäßig klein. Gerade in Kombination mit der Linux-Plattform sind die Hardware-Anforderungen des Servers äußerst gering. Für Wirksysteme, die keine Hochverfügbarkeit erfordern, können deshalb kostengünstige Standard-PCs verwendet werden. Je nach Anzahl der Clients sind dafür auch Systeme älterer Modell-Generationen noch vollständig geeignet.

Die Verwendung einer Linux-Plattform bietet einen weiteren Vorteil, denn der eingesetzte Ubuntu 6.06.1 Server stellt ein vollwertiges Linux auf Basis der Debian-Distribution dar. Damit besteht die Möglichkeit, weitere Netzwerkdienste auf dem selben Host zu integrieren oder Fallback- bzw. Redundanzoptionen auf Dienstebene einzurichten. Das verwendete System bietet mit geringem weiteren Konfigurationsaufwand zusätzlich File-, Print- und Mail-Services sowie weitere gängige Netzwerk-Applikationen wie beispielsweise HTTP-, FTP- und DNS-Server.

Sowohl Ubuntu-Linux als auch OpenVPN sind unter der GNU Public License (GPL) frei verfügbar, so dass keine Kosten für Software-Lizenzen entstehen, ein Vorteil gegenüber Microsoft-Produkten mit vergleichbarem Leistungsumfang. Auf den in hohen Lizenzkosten enthaltenen Supportvertrag mancher Anbieter können und möchten viele Kunden der Zielgruppe der kleinen und mittleren Betriebe oft verzichten.

3. Kalkulation und Beschaffung

3.1 Aufstellung der benötigten Komponenten

Hardware-Komponenten

Es wird ein eigenständiger Server für den Betrieb des VPN-Gateways mit der Zertifizierungsstelle benötigt. Folgende Mindestanforderungen muss der Server erfüllen:

- Prozessor: Intel x86-Plattform, ab 450 MHz
- Arbeitsspeicher: 128 MB
- Festplattenspeicher: 15 GB
- Netzwerkkarte: 100BaseTX Ethernet, RJ45-Anschluss, PCI-Standard
- CD-ROM-Laufwerk, Diskettenlaufwerk

Kleinteile:

- CAT5-Patchkabel

Für die Installation und Konfiguration wird vorübergehend benötigt:

- Standard-Monitor und Tastatur

Software-Komponenten

Das Betriebsystem für den Server:

- Ubuntu Linux, Version 6.06.1 LTS Server (i686)

Zusätzliche Pakete zur Ergänzung der Linux-Grundinstallation:

- build-essential, bin86, make
- LZO-Bibliothek (Echtzeit-Komprimierung)
- libssl (SSL Entwicklungs-Bibliothek)

Die VPN-Anwendung:

- OpenVPN, Version 2.0.9 für Linux
- enthalten ist die OpenSSL-Suite

3.2 Auswahlkriterien und Angebote

Für die Auswahl des zu beschaffenden Servers ergeben sich auf Grundlage des geplanten Einsatzzweckes und einer Dimensionierung, die möglichst gut auf den Kunden zugeschnitten ist, folgende Kriterien.

Hohe Priorität	Niedrige Priorität
geringe Anschaffungskosten	hohe Leistungsreserven
geringer Energieverbrauch	Redundanz kritischer Komponenten
geplante Betriebszeit von 18 Std./Tag	Garantie/Hersteller-Support
hochkompatible Standardkomponenten	Hochverfügbarkeit des Systems

Auf Basis dieser Kriterien und den weiter oben beschriebenen Anforderungen an die Hardware wird entschieden, für die Beschaffung des Servers Gebrauchtgeräte mit in Betracht zu ziehen. Alle auf dem Markt verfügbaren Neugeräte besitzen ein derart hohes Ausstattungsniveau, dass dies nicht als sinnvolle Leistungsreserve betrachtet werden kann, sondern eine unverhältnismä-

ßige Überdimensionierung bedeutet. Zudem sind die Kosten sowohl für die Anschaffung als auch den Energieverbrauch deutlich höher.

In den letzten Jahren hat sich ein professioneller Markt für gebrauchte Computer etabliert. Durch die hohe Fluktuation von PC-Systemen in vielen Großbetrieben wie z. B. Banken oder Versicherungen existiert ein großes Angebot an Gebraucht-PCs, die von guter Qualität und in einem tadellosen Zustand sind, aber von den Betrieben auf Grund eines Wechsels zur nächsten oder übernächsten Gerätegeneration abgestoßen werden. Es gibt zahlreiche gewerbliche Händler, die diese Rechner in größerer Stückzahl aufkaufen, mittels professioneller Diagnose-Werkzeuge testen und schließlich einzeln verkaufen; dafür wird oft das Internetauktionshaus eBay benutzt.

Die hier beschriebenen Angebote sind dadurch gekennzeichnet, dass es sich ausdrücklich um gewerbliche Anbieter handelt und die Gebraucht-PCs zu Festpreisen angeboten werden. Ein weiteres Kriterium für die Auswahl geeigneter Angebote ist der Hersteller. Die Geräte der bekannten großen Markenhersteller wie Hewlett-Packard, Acer, Fujitsu-Siemens oder Maxdata sind überwiegend robuste und funktionale Komplettsysteme, deren Konfiguration (und damit Systemintegrität) während des Einsatzes in den Betrieben in der Regel nicht verändert wurde.

Diese Geräte stellen eine gut geeignete Basis für den zu beschaffenden Server dar. Die Bocom GmbH hat sowohl für frühere Kunden als auch für den Eigenbedarf diverse Systeme aus diesem Marktbereich gekauft und damit gut funktionierende Systeme erstellt. Dadurch sind auch bereits wertvolle Erfahrungen vorhanden, was die Auswahl eines geeigneten Händlers betrifft.

Als zuverlässig haben sich mehrfach die Desktop-PCs von Fujitsu-Siemens erwiesen, die zudem ein gutes Preis-Leistungs-Verhältnis bieten. Die Systeme verwenden ausschließlich Standard-Komponenten, die gut aufeinander abgestimmt sind, hohe Stabilität und angemessene Leistung bieten. Durch ein proprietäres Gehäusekonzept erfolgt die Kühlung der Rechner ausschließlich über den dynamisch geregelten Lüfter des Netzteils, es gibt keine zusätzlichen störanfälligen beweglichen Teile.

Nachfolgend zwei Angebote zur Gegenüberstellung von Gebraucht- und Neukauf. Die ausführlichen Angebote befinden sich im Anhang.

Angebot Gebrauchtware, eBay-Händler	**Angebot Neuware, ALTERNATE GmbH**
Fujitsu Siemens Scenic D i815e MiniDesktop, ATX Prozessor: Intel Pentium III, 1,0 GHz Arbeitsspeicher: 256 MB SDRAM Festplatte: 40 GB, IDE Laufwerke: DVD-ROM, Floppy Grafik: onboard, i815-integrated Netzwerkkarte: onboard, 10/100 Mbps Anschlüsse: 2xPS2, 2xUSB, Par., Ser. Lieferumfang: PC, Stromkabel, Tastatur, Maus Preis: EUR 85,00 inkl. MwSt. + Versandkosten EUR 13,50 = EUR 98,50	Acer Aspire T660 Minitower, ATX Prozessor: Intel Pentium IV, 3,0 GHz Arbeitsspeicher: 512 MB DDR-SDRAM Festplatte: 160 GB, SATA Laufwerke: DVD-DL-RW Grafik: onboard, ATI RC415 integrated Netzwerkkarte: onboard, 10/100 Mbps Anschlüsse: 2xPS2, 6xUSB2.0, Par., Ser. Lieferumfang: PC, Stromkabel, Microsoft Windows Vista Home Basic, Microsoft Works Preis: EUR 489,00 inkl. MwSt. + Versandkosten EUR 12,00 = EUR 501,00

Ausgehend von den in den vorangegangenen Abschnitten beschriebenen Kriterien fällt die Entscheidung auf den preiswerten Gebraucht-PC von Fujitsu-Siemens. Dieser wird im Auftrag des Kunden beschafft und zur Installation vom Händler direkt an die Bocom GmbH geliefert.

3.3 Die notwendigen Internetanbindungen

Für das angebotene VPN wird das Internet als Transportmedium benutzt. Zwar unterliegen die effektiven Datendurchsatzraten potentiellen Schwankungen, die durch das dynamische Traffic-Aufkommen verursacht werden, das außerhalb des eigenen Einflussbereichs liegt – es kann jedoch mit der Wahl einer möglichst hohen Bandbreite für die bestehenden ADSL-Anschlüsse eine angemessene Ausgangssituation für einen möglichst komfortablen VPN-Betrieb geschaffen werden.

Am Standort des Servers wird ein Upgrade des vorhandenen T-DSL-Business 2000-Anschlusses auf einen ADSL2+-Zugang mit 16 Mbps im Downstream und 1 Mbps im Upstream durchgeführt. Der wichtigste Grund hierfür ist die Erhöhung des Upstreams, da in vielen Anwendungsbereichen Daten vom Server geholt werden und diese also durch den VPN-Tunnel über das Internet zu den Clients geschickt werden müssen.

Am Standort des Heimarbeitsplatz-PCs wird für den vorhandenen T-DSL-Anschluss ein Upgrade auf 6 Mbps im Downstream und 512 Kbps im Upstream beauftragt.

Die existierenden Flatrate-Tarife sind mit den neuen Bandbreiten der DSL-Leitungen verwendbar und müssen nicht geändert werden. Die FRITZ!Box am Standort des Büro-Intranets läuft bereits unter der aktuellen Firmware-Version und ist damit ADSL2+-kompatibel.

3.4 Kostenkalkulation in tabellarischer Übersicht

		Einzelpreis	Gesamtpreis
Materialkosten			
1 x	Gebraucht-PC FSC Scenic L i815 (eBay-Händler)	85,00 €	85,00 €
1 x	Versandkosten Lieferant	13,50 €	13,50 €
1 x	Netzwerkkabel CAT5 STP, 10 m	7,50 €	7,50 €
Summe Materialkosten			106,00 €
Fertigungskosten			
26 x	Arbeitslohn Bocom GmbH IT-Azubi	45,00 €	1.170,00 €
2 x	Fahrtkosten-Pauschale Regionalbereich	30,00 €	60,00 €
Summe Fertigungskosten			1.230,00 €
Summe Herstellkosten = Material- + Fertigungskoten			**1.336,00 €**
Zuschlag Verwaltungsgemeinkosten (10 %)			+ 133,60 €
Zuschlag Vertriebsgemeinkosten (10 %)			+ 133,60 €
Summe Selbstkosten			**1.603,20 €**
Gewinnzuschlag (10 %)			+ 160,32 €
Gesamtpreis netto			1.763,52 €
Umsatzsteuer (19 %)			335,07 €
Gesamtpreis brutto			**2.098,59 €**

Auf Grundlage dieser Kostenkalkulation erstellt die Bocom GmbH ein Angebot, das per Telefax an die Baumann Immobilien geschickt wird. Am nächsten Tag meldet sich Herr Baumann telefonisch und erkundigt sich über bestimmte Details sowie den möglichen Ablauf. Noch am selben Tag erhält die Bocom GmbH ein Telefax von Frau Baumann als schriftliche Bestellung.

Damit der Auftrag ordnungsgemäß dokumentiert ist, wird im Auftrag der Bocom GmbH eine schriftliche Auftragsbestätigung erstellt und per Post an den neuen Kunden versendet.

4. Installation und Konfiguration

4.1 Installation Phase I – Durchführung im eigenen Betrieb

4.1.1 Betriebssystem-Installation des VPN-Servers

Die Vorgehensweise zur Einrichtung des Ubuntu Linux wird im folgenden anhand der wichtigsten Punkte erläutert.

Für die Installation des Betriebssystems wird der Ubuntu Server in der Version 6.06.1 LTS von der Ubuntu-Webseite in Form einer ISO-Datei heruntergeladen. Anschließend kann mit einem Brennprogramm die Installations-CD erstellt werden. Nachdem der Server mit dieser CD gebootet wurde, bietet das Boot-Menü die Auswahl zwischen zwei Installationstypen: es kann ein absolutes Basissystem gewählt werden oder eine so genannte LAMP-Version (= Linux Apache MySQL PHP). Da es keine Nachteile hat, diese Standard-Dienste eines Linux-Systems während der Installation gleich mit einzurichten, wird die LAMP-Version gewählt.

Die Festplatte wird wie folgt eingeteilt:

0,5	GB	swap	Auslagerung
10	GB	`/`	Root-Partition
10	GB	`/home`	User-Verzeichnisse
19,5	GB	`/storage`	Zusatzpartition für separaten Speicherplatz

Im weiteren Verlauf des Installationsprogramms werden noch einige wenige Grundeinstellungen wie u.a. Hostname und Netzwerkeinstellungen abgefragt.

Nach Abschluss der Installation und des ersten Starts von der Festplatte wird eine Aktualisierung des Systems zur Installation von Updates und Patches durchgeführt. Dazu kommt das Paketmanagement-System „Advanced Packaging Tool“ (APT) zum Einsatz, das der Standard für alle Debian/GNU basierten Linux-Versionen ist. Mithilfe dieses Programms werden auf dem System nicht nur alle erforderlichen Aktualisierungen der installierten Softwarepakete durchgeführt, sondern ebenso ein Update des verwendeten Linux-Kernels installiert.

Im Anschluss werden mit dem APT die für die Grundausstattung noch benötigten Pakete „build-essential“, „bin86“ und „make“ installiert. Ebenso die Entwicklungs-Bibliothek „libssl-dev“ für die von OpenVPN verwendete OpenSSL-Suite. Die für OpenVPN benötigte Echtzeit-Komprimierung LZO wird als Quelltext-Version aus dem Internet heruntergeladen, entpackt, kompiliert und installiert.

Damit ist das Grundsystem vollständig installiert.

4.1.2 Installation der VPN-Anwendung

Um das aktuellste Release von OpenVPN zu erhalten wird zur Installation nicht APT benutzt, sondern die Quelltext-Version von der Webseite www.openvpn.net heruntergeladen und entpackt. Die Kompilierung und das Installieren mit den mitgelieferten Skripten **`configure`** und **`make`** erfolgt mit den Standardeinstellungen und bedarf keiner zusätzlichen Parameter. Das Programm wird in das Verzeichnis **`/usr/local/bin/openvpn`** installiert, sämtliche Konfigurationsdateien werden in **`/etc/openvpn`** abgelegt. Es wird ein Benutzer-Account „ovpn“ und die Gruppe „ovpn“ angelegt, unter dem der OpenVPN Daemon (= Systemdienst unter Linux) später ausgeführt wird (s.u.). Dem neu angelegten Benutzer wird mittels des **`chown`**-Befehls der Besitz an den beiden für OpenVPN erstellten Verzeichnissen und allen enthaltenen Dateien und Unterverzeichnissen übertragen.

Anmerkungen zur Public Key Infrastruktur (PKI)

Für die Verschlüsselung des VPN-Tunnels verwendet OpenVPN das Transport Layer Security-Protokoll (TLS), welches aus Sicht des OSI-Referenzmodells zwischen der Schicht 4 – Transportschicht – und den Anwendungsschichten arbeitet. Damit ist es sowohl unabhängig von dem verwendeten Transportprotokoll (TCP oder UDP) als auch transparent für die Protokolle der Anwendungsschichten 5 bis 7.

Für die Authentisierung und Authentifizierung sollen so genannte selbst signierte Zertifikate benutzt werden. Dieses Verschlüsselungsverfahren ist ein asymmetrisches Verfahren, d. h. für Ver- und Entschlüsselung werden unterschiedliche Schlüssel benutzt. Dies wird auch als Public-Key-Methode bezeichnet. Für jeden Kommunikationsteilnehmer gibt es jeweils einen öffentlichen, nicht geheimen, sowie einen privaten, geheimen Schlüssel. Der öffentliche Schlüssel eines Teilnehmers wird von allen anderen zum Verschlüsseln der an ihn gerichteten Nachrichten verwendet. Die Dekodierung kann nur mit dem privaten Schlüssel erfolgen. Um sicherzustellen, dass ein bestimmter öffentlicher Schlüssel zu dem angenommenen Eigentümer gehört, werden in einer PKI Zertifikate verwendet, die Prüfsummen und Angaben über die Gültigkeit enthalten.

Als Referenzpunkt hierfür dient eine so genannte Zertifizierungsstelle (CA = Certificate Authority), die nach Überprüfung der Identität Zertifikate ausstellt. Für den öffentlich zugänglichen Betrieb, beispielsweise im Internet, gibt es kommerzielle und freie CAs, die Zertifizierungsanfragen entgegennehmen und bei Identitätsnachweis signieren, also den öffentlichen Schlüssel des Anfragenden als geprüft und gültig deklarieren. In geschlossenen Systemen wie einem VPN wird eine eigene CA eingerichtet, die benötigten Schlüssel werden also selbst signiert.

OpenVPN verwendet für die Implementierung des TLS-Protokolls die als Open-Source unter der Apache-Lizenz (APL) frei verfügbare OpenSSL-Suite. Für die komfortable Bedienung von OpenSSL bringt das OpenVPN-Paket eine Reihe von Skripten mit (zusammengefasst unter dem Namen „easy-rsa“), die es ermöglichen, auf einfache Weise die für jeden VPN-Client und den Server benötigten privaten Schlüssel und Zertifikate zu erstellen und zu signieren.

Einrichtung der PKI mithilfe der „easy-rsa“-Skripte

Zunächst werden in der Datei **`/easy-rsa/vars`** die Standardwerte für die zu erstellenden Zertifikate angepasst, dies sind Angaben, welche die Herkunft der Zertifikate beschreiben, also über die Zertifizierungsstelle informieren (z. B. Provinz, Stadt, E-Mail-Adresse, u.a.). Anschließend wird die Datei als Skript ausgeführt, damit werden die eingetragenen Standardwerte bei den nächsten Schritten verwendet.

Durch das Ausführen des Skriptes **`clean-all`** werden alle womöglich existierenden Schlüssel gelöscht und schließlich über **`build-ca`** die Zertifizierungsstelle eingerichtet. Dieses Skript erzeugt die Wurzel (den Referenzpunkt) der eigenen PKI in Form eines öffentlichen und privaten Schlüssels. Anschließend wird mit **`build-key-server`** das Schlüsselpaar für den VPN-Server

erzeugt. Damit ist die Serverinstanz in der Lage, Verbindungsanfragen entgegen zu nehmen und auf ihre Echtheit und die Zugriffsberechtigung im Sinne der PKI zu validieren, d. h. die Client-Anfrage zu authentifizieren.

Für jeden Client wird nun mit dem Skript **`build-key`** und dem angehängten Parameter **`client01`**, **`client02`**, usw. ebenfalls ein Schlüsselpaar generiert. Dabei werden für das Ausfüllen der Zertifikatsfelder die vorgegebenen Werte aus der Datei **`easy-rsa/vars`** benutzt (s.o.). Entscheidend für die Individualisierung und Eindeutigkeit der erzeugten Zertifikate ist das Feld „CN“ (= Common Name), in das ein clientspezifischer Name bzw. eine fortlaufende Nr. o.ä. eingetragen wird.

Als zusätzliches Sicherheitsfeature wird ein verschlüsselter so genannter „Message Authentication Code“ (MAC) erzeugt, der zur Prüfung der Integrität und Authentizität der verschickten Datenpakete verwendet wird. Damit kann sichergestellt werden, dass die übertragenen Daten auf ihrem Weg durch das Netzwerk nicht verändert werden, vereinfacht ausgedrückt ist es eine Art zusätzliche Prüfsumme, die durch einen Schlüssel berechnet wird; dieser wird allen beteiligten Kommunikationspartnern zur Verfügung gestellt. Dadurch wird bereits der Verbindungsaufbau von TLS-Verbindungen zusätzlich abgesichert. Erstellt wird die Schlüsseldatei mit dem Befehl **`openvpn --genkey --secret ta.key`**.

Außerdem muss noch eine Datei mit den Parametern für das Diffie-Hellman-Protokoll (DH) erstellt werden. Dieses wird von dem OpenVPN-Server für den Austausch der Schlüssel mit den Clients verwendet. Das DH-Protokoll gehört zur Familie der Key-Agreement-Protokolle (Schlüsselaustausch-Protokolle) und bietet mit seinen Algorithmen zwei Kommunikationspartnern die Möglichkeit, durch den Austausch einer Nachricht über einen unsicheren Kanal einen gemeinsamen geheimen Schlüssel für eine Sitzung (einen Session Key) zu erzeugen. Das entsprechende Skript zur Erstellung der Parameter-Datei lautet **`build-dh`**. Da keine weiteren Parameter angegeben werden, wird die Schlüssellänge auf 1024 bit festgelegt.

Abschließend liegen folgende Dateien vor, die wie in der Tabelle angegeben, verteilt werden müssen.

Dateiname	Verwendungszweck	wird benötigt von	geheim
`ca.crt`	Zertifikat der CA (Referenz)	Server, alle Clients	Nein
`ca.key`	Privater Schlüssel der CA	Zertifizierungsstelle	Ja
`dh1024.pem`	DH-Parameter	Server	Nein
`server.crt`	Zertifikat des Servers	Server	Nein
`server.key`	Privater Schlüssel des Servers	Server	Ja
`client01.crt`	Zertifikat des Client 1	Client 1	Nein
`client01.key`	Privater Schlüssel des Client 1	Client 1	Ja
`client02.crt`	Zertifikat des Client 2	Client 2	Nein
`client02.key`	Privater Schlüssel des Client 2	Client 2	Ja

Die Konfigurationsdatei für den OpenVPN-Server

Nachfolgend die wichtigsten Merkmale der Konfigurationsdatei **`baumann.conf`** des Servers. Die vollständige Konfiguration befindet sich im Anhang.

- der Server hört den Port 1194/UDP ab
- es wird das Subnetz 192.168.92/24 für das VPN verwendet
- die Clients erhalten eine Route in das Intranet (192.168.82.0/24)
- und die IP-Adresse des WINS-Servers für die Namensauflösung (192.168.82.10)
- die Kommunikation zwischen den VPN-Clients wird erlaubt

Einrichtung des OpenVPN-Dienstes

Der Server wird so eingerichtet, dass OpenVPN als Daemon im Hintergrund läuft und beim Hochfahren des Servers automatisch gestartet wird. In dem Verzeichnis **`/etc/init.d`** wird ein Startskript **`openvpn.sh`** angelegt. Da das Ubuntu-Linux für den regulären Betrieb das Runlevel 2 verwendet, wird eine entsprechende Verknüpfung in dem Verzeichnis **`/etc/rc2.d`** angelegt. Da der Server wie weiter oben erläutert den Clients eine Route in das Intranet zur Verfügung stellt, muss zudem die Routing-Funktionalität, das IP-Forwarding, über das Startskript aktiviert werden.

Das Startskript openvpn.sh:

```
#!/bin/sh
/usr/local/bin/openvpn/openvpn --daemon --config /etc/openvpn/baumann.conf
echo 1 > /proc/sys/net/ipv4/ip_forward
```

4.1.3 Das Installationspaket für die Systemadministratorin

Da die Administratorin der Baumann Immobilien Frau Mohn nur zeitweise vor Ort ist, wird ein Installationspaket für ihren entfernten Rechner zusammengestellt, das sie bei nächster Gelegenheit mitnehmen kann. Folgende Daten werden dazu auf eine CD gebrannt:

- openvpn-2.0.9-install.exe (OpenVPN-Version für Windows 2000/XP)
- bmimmoclient.ovpn (fertige Client-Konfigurationsdatei)
- ca.crt (der public key der Zertifizierungsstelle)
- ta.key (der Schlüssel für die MAC-Berechnung)
- client03.key (der private Schlüssel für Frau Mohns Client)
- client03.crt (das Zertifikat für Frau Mohns Client)

Da im Rahmen des Projektes kein Merkblatt für die Administratorin erstellt werden kann, wird vereinbart, dass die Bocom GmbH bei möglichen Installationsproblemen kostenlosen telefonischen Support leistet.

4.2 Installation Phase II – Vor-Ort-Installation beim Kunden

4.2.1 Aufstellen und Inbetriebnahme des Servers

Der vorinstallierte Server wird in dem Kellerraum des Bürogebäudes der Baumann Immobilien aufgestellt, in dem sich bereits alle Netzwerk-Komponenten des Intranets sowie der Domänen-Controller befinden. Folgende Schritte sind durchzuführen:

- statische IP-Konfiguration der Netzwerkkarte über die Datei **`/etc/network/interfaces`**
  IP-Adresse 192.168.82.8, Subnetzmaske 255.255.255.0
  Standard-Gateway 192.168.82.1, Netzwerkadresse 192.168.82.0
  Broadcast-Adresse 192.168.82.255, Hostname ubuntu
- Eintragen der IP-Adresse der FRITZ!Box als DNS-Server in der Datei **`/etc/resolv.conf`**
- Verbinden der Netzwerkkarte mit einem Port des Netgear-Switches

4.2.2 IP-Konfiguration des Intranets

Die Intranet-Clients erhalten zur besseren Administrierbarkeit statische IP-Adressen, damit die Systemadministratorin die Rechner auch beim Ausfall des Namensauflösungs-Dienstes unkompliziert erreichen kann, die Verwendung von DHCP (= Dynamic Host Configuration Protocol)

bietet in einem Netzwerk dieser verhältnismäßig geringen Größe keine nennenswerten Vorteile. Die vergebenen Adressen können dem Netzwerkplan (s. Anhang) entnommen werden.

In dem gleichen Arbeitsschritt wird die IP-Adresse des Domänen-Controllers als WINS-Serveradresse in die Netzwerkeinstellungen der Clients eingetragen. Um die Einrichtung der WINS-Konfiguration abzuschließen, wird nun auf dem Windows NT-Server auf der Registerkarte „Dienste“ in der Netzwerk-Konfiguration der „WINS-Dienst“ hinzugefügt. Dafür muss bei entsprechender Aufforderung einmalig die Windows NT Server-CD eingelegt und schließlich der Rechner neu gestartet werden. Weitere Konfigurationsschritte sind nicht erforderlich.

Wie bereits bei der Beschreibung der Konfigurationsdatei des VPN-Servers erwähnt, erhalten die VPN-Clients über eine Route Zugriff auf das Intranet, der OpenVPN-Server routet also vom VPN-Subnetz in das interne Netz. Damit die Kommunikation jedoch funktioniert, muss der Weg in die andere Richtung ebenso bekannt sein. Dies lässt sich mit einem Eintrag für eine statische Route auf der FRITZ!Box (das Standard-Gateway für das Intranet) erreichen. Unter dem Menüpunkt „System > Netzwerkeinstellungen“ des Web-Interfaces wird über den Button „IP-Routen“ folgender Routing-Eintrag vorgenommen:

Netzwerk 192.168.92.0Netzwerkmaske 255.255.255.0, Gateway 192.168.82.8

Damit der OpenVPN-Server aus dem Internet erreichbar ist, erfolgt eine Anmeldung bei dem für die gewünschten Funktionen kostenfreien Dienst DynDNS.org. Dort wird der DNS-Name „bmimmo44021.dyndns.org“ (Name aus Datenschutzgründen geändert) registriert. Mittels des in der FRITZ!Box integrierten Clients wird die für den Namen hinterlegte IP-Adresse automatisch aktualisiert, sobald diese sich durch die Wiedereinwahl ins Internet ändert. Dafür werden die Zugangsdaten des DynDNS-Accounts und der registrierte Hostname über das Web-Interface in dem DSL-Router gespeichert. Damit die FRITZ!Box die Anfragen der OpenVPN-Clients an den Server weiterleitet, wird der Port 1194/UDP auf die IP-Adresse des Ubuntu-Systems umgeleitet.

Die Anpassung des Intranets ist damit vollständig abgeschlossen.

4.2.3 Einrichten des VPN-Clients

Das Projekt umfasst die Anbindung von zwei Clients. Da sich die Einrichtung von OpenVPN auf den einzelnen Clients jedoch nicht unterscheidet, wird die entsprechende Vorgehensweise im folgenden Abschnitt einmal dokumentiert.

Die OpenVPN-Version für die Microsoft-Plattform läuft unter Windows 2000, XP und 2003. Die benötigte Datei wird von der OpenVPN-Website heruntergeladen, es handelt sich um eine EXE-Datei, die einen vollständigen Installations-Assistenten mitbringt. Für die Installation können die Standardeinstellungen benutzt werden. Während des Installationsprozesses wird ein virtueller Netzwerktreiber installiert, der im System als ein zusätzlicher Netzwerkadapter eingebunden und dargestellt wird. Nach Abschluss der Installation liegt das Programm im Verzeichnis **`%SYSTEMROOT%\Programme\OpenVPN`** und kann konfiguriert werden, eine grafische Benutzeroberfläche wird nicht mitgeliefert. Sollte eine Personal Firewall auf dem Rechner verwendet werden, so sind sämtliche Kontrollmechanismen für die virtuelle Netzwerkkarte abzuschalten. Es entsteht kein Sicherheitsrisiko, da sämtlicher Netzwerkverkehr, der über diesen Adapter transportiert wird, bereits durch OpenVPN authentifiziert wurde.

Nun wird in dem OpenVPN-Ordner ein Unterverzeichnis **`keys/`** angelegt und das Schlüsselpaar des Clients sowie der öffentliche Schlüssel der Zertifizierungsstelle und der MAC-Schlüssel dort abgelegt. Die Client-Konfigurationsdatei **`bmimmoclient.ovpn`** wird in das existierende Unterverzeichnis **`config/`** kopiert.

Schließlich wird die Windows-Diensteverwaltung über Start > Systemsteuerung > Verwaltung > Dienste geöffnet und in den Eigenschaften des bereits vorhandenen Dienstes „OpenVPN

Service“ die Startart auf „Automatisch“ gesetzt. Damit wird OpenVPN beim Windows-Start automatisch im Hintergrund ausgeführt und erstellt für jede im Ordner `config` vorhandene `.ovpn`-Datei eine OpenVPN-Instanz.

4.2.4 Funktionstest

Um das Gesamtsystem auf seine ordnungsgemäße Funktion zu überprüfen, werden von allen beteiligten Rechnern aus ausführliche Tests mit dem ICMP-Tool `ping` gemacht. Mittels der versendeten Echo-Anforderungen und empfangenen Antworten kann einfach geprüft werden, ob die Netzwerkkonfiguration stimmt und das Routing funktioniert.

In einem weiteren Test wird die Keep-Alive-Funktion der VPN-Teilnehmer geprüft. Diese sorgt dafür, dass nach einer Trennung der verwendeten Netzwerkverbindung anschließend die VPN-Verbindung automatisch wiederhergestellt wird. Dafür wird bei den VPN-Clients zu Testzwecken im laufenden Betrieb das Netzwerkkabel entfern und wieder verbunden. Außerdem wird der OpenVPN-Daemon auf dem Server wiederholt gestoppt und gestartet sowie der Rechner neu gebootet, um die automatische Wiedereinwahl der Clients zu prüfen.

Alle Test verlaufen erfolgreich, die VPN-Konnektivität funktioniert.

5. Projektabschluss

5.1 Datensicherung der erstellten Konfiguration

Nach Abschluss der gesamten Installations- und Konfigurationsarbeiten wird eine Datensicherung sämtlicher individueller Dateien zusammengestellt und auf CD gebrannt. Dazu zählen neben allen Schlüsseldateien und Zertifikaten der PKI die OpenVPN-Konfigurationsdateien und die auf dem Server erstellten Skripte.

Außerdem wird die Konfiguration der FRITZ!Box in eine Datei gesichert und dem Backup hinzugefügt. Es werden zwei Exemplare der CD gebrannt, eine wird in dem feuerfesten Aktensafe im Büro der Buchhalterin hinterlegt, die andere lagert der Geschäftsführer in seinen Privaträumen.

5.2 Übergabe des Systems an den Kunden

Zum Abschluss des Projektes findet die Übergabe des Systems an den Kunden statt. In einer kurzen Besprechung mit Herrn Baumann und Frau Mohn werden noch einmal alle durchgeführten Arbeiten reflektiert und kurz erläutert. Der Kunde wird darauf hingewiesen, dass das Gesamtsystem keine Einrichtungen zur Ausfallsicherheit besitzt. Weder die Netzwerkanbindung noch die Server-Hardware ist redundant ausgelegt. Zwar ist dies auch zum jetzigen Zeitpunkt nicht gefordert, die Bocom GmbH hält es jedoch für wichtig, nochmals darauf hinzuweisen. Die Erfahrung hat gezeigt, dass sich viele Anwender schnell an die durch das VPN gebotene Konnektivität gewöhnen und diese unbewusst als ständig verfügbar einordnen.

Schließlich wird der Kunde noch darauf aufmerksam gemacht, dass es hinsichtlich des Datendurchsatzes bestimmte Einschränkungen gibt. Für viele Anwendungen ist vorhandene Bandbreite ausreichend, es muss aber bedacht werden, dass der Transfer größerer Dateien (ab ca. 5 MB) deutlich mehr Zeit in Anspruch nehmen als im Intranet.

Der Systemadministratorin Frau Mohn werden für die Fernwartung freie VNC-Tools (= Virtual Network Computer) wie z.B. RealVNC empfohlen, mit denen Rechner über ein Netzwerk ferngesteuert werden können. In Verbindung mit der WakeOn-LAN-Funktion, die viele PCs bieten, kann damit eine quasi autonome Fernwartung durchgeführt werden, da die Rechner aus der Ferne über das Netz eingeschaltet werden. können.

Der Kunde äußert seine Zufriedenheit über die gute Zusammenarbeit und das erhaltene System. Für optionale Erweiterungen wird er sich bei Bedarf erneut an die Bocom GmbH wenden.

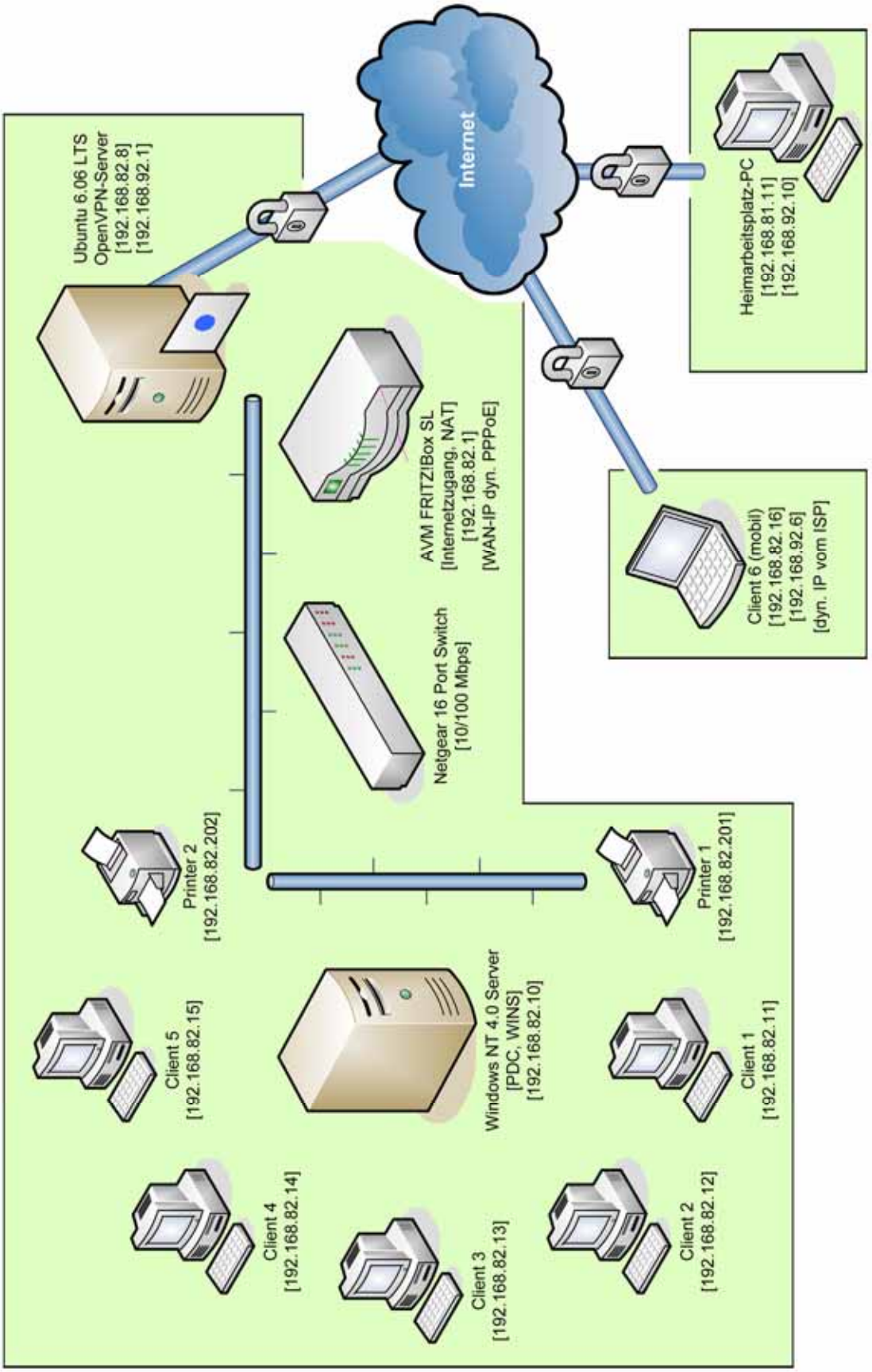
5.3 Schlussbemerkungen

Auf Grund meiner angeborenen Visus-Einschränkung bin ich in bestimmten Arbeitsbereichen auf unterstützende Assistenz angewiesen. Dies betrifft insbesondere die Installationsarbeiten vor Ort beim Kunden, wie etwa die Verkabelung von Komponenten oder die kurzfristige Bedienung von Kunden-Systemen, deren Anzeige-Eigenschaften nicht auf meine speziellen Bedürfnisse eingestellt sind. Ebenso sind An- und Abfahrten, die zwecks Transport von Material oder der Erreichbarkeit nur mit dem Auto erfolgen können für mich nur mit einem Fahrer möglich.

Daher arbeite ich bei praktischen Tätigkeiten häufig mit einem Kollegen zusammen, so dass es in der Regel keine vermeidbaren Probleme diesbezüglich gibt – die Arbeit im Team besitzt naturgemäß auch generelle Vorteile.

6. Anhang

6.1 Netzwerkplan Baumann Immobilien



6.2 Angebote für die Server-Hardware

6.2.1 Angebot Gebrauchtware, eBay-Händler

Kategorie: Computer > PC-Systeme > Desktop- & Tower-PC > Ab 1 GHz > Intel

Fujitsu Siemens Scenic D P3 1.0GHz (Rechnung & Gewähr) Artikelnummer: 250102167030

Sofort Kaufen Preis: **EUR 85,00** inkl. MwSt.

Versandkosten: **EUR 13,50** Versicherter Versand Service nach: Deutschland

Versand nach: Deutschland

Artikelstandort: Bramsche, Deutschland

Menge: 10 von 10 verfügbar

Angebotsende: **16.04.07 14:38:11 MESZ** (1 Tag 2 Stunden)

Übersicht: Abgeschlossene Transaktionen aufrufen

Verkäufer: www_mrw-distribution_de (893) mich

Bewertung: **893 (100% positiv)**

Mitglied: seit 09.10.02 in Deutschland

Verpackung und Versand

Sparen Sie Versandkosten –kaufen Sie jetzt weitere Artikel dieses Verkäufers!
Versandrabatte werden direkt vom Verkäufer angeboten. Weitere Informationen finden Sie möglicherweise in der Artikelbeschreibung.
Bestimmte Artikel sind möglicherweise ausgeschlossen.

Versand nach
Deutschland

Land: Alle verfügbaren anzeigen

Verpackung und Versand	Jeder weitere Artikel	Nach	Service
EUR 13,50	+ EUR 6,50	Deutschland	Versicherter Versand
EUR 17,50	+ EUR 6,50	Deutschland	Nachnahme (Versand inkl. Nachnahmegebühr)

Der angegebene Preis enthält die gesetzliche Mehrwertsteuer.
Wenn Sie Fragen zur ausgewiesenen Mehrwertsteuer haben, wenden Sie sich bitte an den Verkäufer. Bei internationalen Verkäufen gelten die gesetzlichen Bestimmungen.

Rücknahme

Rücknahme - Weitere Angaben:	Rücksendung / Rücktritt vom Kaufvertrag / Wiederrufsbelehrung Widerrufsrecht: Sie können Ihre Vertragserklärung innerhalb von einem Monat ohne Angabe von Gründen in Textform (z. B. Brief, Fax, EMail ebay@mrw-distribution.de) oder durch Rücksendung der Sache widerrufen. Die Frist beginnt frühestens mit Erhalt der Ware und der Belehrung in Textform. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs oder der Sache. Der Widerruf ist an folgende ladungsfähige Anschrift für gerichtliche Schriftstücke zu richten: MRW MediaDesign & Distribution - RÜCKTRITT EBAY - Elbestr. 9 49565 Bramsche Widerrufsfolgen: Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren und ggf. gezogene Nutzungen (z. B. Zinsen) herauszugeben. Können Sie uns die empfangene Leistung ganz oder teilweise nicht oder nur in verschlechtertem Zustand zurückgewähren, müssen Sie uns insoweit ggf. Wertersatz leisten. Bei der Überlassung von Sachen gilt dies nicht, wenn die Verschlechterung der Sache ausschließlich auf deren Prüfung -- wie sie Ihnen etwa im Ladengeschäft möglich gewesen wäre -- zurückzuführen ist. Im Übrigen können Sie die Wertersatzpflicht vermeiden, indem Sie die Sache nicht wie ein Eigentümer in Gebrauch nehmen und alles unterlassen, was deren Wert beeinträchtigt. Hierzu gehören auch evtl. Zubehörteile, Handbücher, Kartonage, etc. und insbesondere Software. Paketversandfähige Sachen sind zurückzusenden. Bei einer Rücksendung aus einer Warenlieferung, deren Bestellwert insgesamt bis zu 40 Euro beträgt, haben Sie die Kosten der Rücksendung zu tragen, wenn die gelieferte Ware der bestellten entspricht. Anderenfalls ist die Rücksendung für Sie kostenfrei. Nicht paketversandfähige Sachen werden bei Ihnen abgeholt. Ein Widerrufsrecht besteht nach den gesetzlichen Vorgaben unter anderem nicht bei - Lieferung von Computersoftware in versiegelten Packungen, wenn das Siegel von Ihnen geöffnet wurde - Lieferung von Produkten, die nach Kundenspezifikationen angefertigt werden oder eindeutig auf die persönlichen Bedürfnisse zugeschnitten sind oder die auf Grund ihrer Beschaffenheit nicht für eine Rücksendung geeignet sind. Bitte legen Sie zum Paket unbedingt eine Rechnungskopie oder einen Ausdruck der Auktion sowie Ihre aktuelle Bankverbindung für die Rücküberweisung.

Verbraucher haben das Recht, den Artikel unter den angegebenen Bedingungen zurückzugeben.

Einzelheiten zur Bezahlung

Zahlungsmethode

Überweisung

Barzahlung bei Abholung

Nachnahme

Beschreibung

Der Verkäufer ist verantwortlich für das Angebot.

Artikelmerkmale - PC-Systeme

Zustand:	**Gebraucht**	Festplattenkapazität:	**40 GB**
Bauart:	**Desktop-PC**	Internes Laufwerk:	**DVD-ROM**
Marke:	**Fujitsu-Siemens**	Modell Grafikkarte:	**--**
Prozessortyp:	**Intel Pentium III**	Ausstattungsmerkmale:	**Netzwerkkarte, USB 1.1**
Prozessorgeschwindigkeit:	**1.000 MHz**	Peripheriegeräte:	**Maus, Tastatur**
Arbeitsspeicher (RAM):	**256 MB**		

MRW MediaDesign & Distribution

Neu- & Gebraucht EDV-Waren: PC-Systeme (ab PIII) | **Monitore/TFTs** | **Drucker** (Laser/Ink) | **Scanner**

vieles mehr...

PC-Systeme: Intel Pentium 3

Art-Nr.:1064

Fujitsu Siemens Scenic D i815e

Fujitsu Siemens richtet ein besonderes Augenmerk auf die sorgfältige Auswahl und Qualifizierung seiner Lieferanten sowie die Einhaltung aller internationalen Standards. Daneben werden sämtliche Komponenten sowie das Gesamtsystem vor ihrer Auslieferung umfassenden Funktionstests unterzogen.

Gerätetyp	MiniDesktop ATX
Prozessorleistung	Intel Pentium III 1.0GHz
Arbeitsspeicher	256 MB (SDR)
Massenspeicher	40 GB (IDE)
Laufwerke	DVD-ROM, FDD
Grafik	onboard
Sound	onBoard
LAN	onBoard (10/100)
Anschlüsse	2xPS2, 2xUSB, Parallel, Serial
Abmessungen [Netto]	375x440x105 mm (BxTxH)
Gewicht [Netto]	ca. 8,00 Kg
Spannungsversorgung	230 Volt
Lieferumfang	Stromkabel, Tastatur, Maus

Kundeninformation/Ergänzungen:
keine

Allgemeine Geschäfts- und Lieferbedingungen für die Plattform eBay

- Bei der Ware, auf die Sie hier bieten, handelt es sich um gebrauchte Ware. Diese kann somit Gebrauchsspuren aufweisen. Der angebotene Artikel wurde auf seine Funktion getestet und gereinigt. Software oder Handbücher sind, falls nicht anders beschrieben, nicht Bestandteil dieser Auktion.
- Nach Beendigung der Auktion erhalten Sie innerhalb eines Werktages eine E-Mail mit Zahlungsinformationen.
- Nach Zahlungseingang wird die Ware über DHL oder GLS als versichertes Packet an die von Ihnen genannte Adresse versandt. (Versicherung in Höhe des Warenwertes bis max. 500 €)
- Akzeptierte Zahlungsmethoden: Vorkasse, Nachnahme und Barzahlung.
- Die Ware bleibt bis zur vollständigen Zahlung unser Eigentum.
- Auf ersteigerte Artikel wird ein Monat Rückgaberecht gewährt.
- Sofern Sie von dem Rückgaberecht Gebrauch machen, wird nach Rückerhalt der Ware der volle Kaufbetrag zurücküberwiesen.
- Bei Reklamationen in der Gewährleistungszeit von 12 Monaten (Privatpersonen) wird der erworbene Artikel nach Prüfung der Technik repariert, ausgetauscht oder der Kaufwert erstattet.
- Geringfügige Abweichungen von der Abbildung sind vorbehalten.
- Vollständigkeit und Unversehrtheit der Ware ist im Beisein des Anlieferers zu überprüfen. Bei auftretenden Mängeln sind diese innerhalb von 3 Werktagen nach Erhalt der Ware zu melden.
- Garantieaustausch nur mit RMA-Nummer. RMA Antrag bitte per E-Mail anfordern.

Salvatorische Klausel
Sollte eine der Bestimmungen dieser Allgemeinen Geschäftsbedingungen unwirksam sein oder werden, so berührt dies die Wirksamkeit der AGB im Übrigen nicht.

Mit Abgabe Ihres Gebotes, erklären Sie sich mit den Allgemeine Geschäfts- und Lieferbedingungen einverstanden.

Sie erhalten eine Rechnung mit ausgewiesener Mehrwertsteuer und 12 Monate Gewährleistung.

Erstellt durch eBay Turbo Lister

00161
Mehr zum Thema eBay-Besucherzähler

Rechtliche Informationen des Verkäufers

MRW MediaDesign & Distribution Inh.
Markus Windisch
Markus Windisch
Elbestr. 9
49565 Bramsche
Deutschland

Telefon: 054613682
Fax: 05461886312
E-Mail: webmaster@barebonecosmetix.de

Siehe MICH-Seite

Umsatzsteuer-Identifikationsnummer: DE 234590094
Die Mehrwertsteuer wird auf meinen Rechnungen separat ausgewiesen.

Widerrufs- oder Rückgabebelehrung
Siehe Informationen zu den Rücknahmebedingungen des Verkäufers unten: Angaben zu Zahlung, Versand und Rücknahme

Allgemeine Geschäftsbedingungen
Angaben zum Unternehmen: Name: MRW MediaDesign & Distribution Anschrift: Elbestr. 9, 49565 Bramsche Telefon: +49 5461 3682 Fax: +49 5461 886312 Mobile: 0171 4724096 Email: windisch@mrw-distribution.de, windisch@mrw-mediadesign.de Inhaber: Markus Windisch Inhalt: Markus Windisch Steuernummer: 67/148/01223 USt - IdNr: DE234590094 ---------- Versand: Wir verschicken unsere Waren ausschliesslich mit der Deutschen Post AG! (DHL) und General Logistics Systems (GLS), sofern es nicht anderes in der Auktion definiert ist. Das hat für Sie den großen Vorteil, dass das Paket innerhalb einer Woche in Ihrer Postfiliale (DHL) abgeholt werden kann. Jedes Paket wird automatisch bis 500,- EUR versichert. ---------- Lagerware: Alle Artikel die auf EBAY angeboten werden, sind direkt verfügbar. Lieferung so lange Vorrat reicht. Änderungen und Irrtümer ausgeschlossen. Auktionsbilder können Symbolbilder sein. Der Lieferumfang wird schriflich in der Auktion, sofern nicht dann in den AGB's, definiert. ---------- Rechnung: Sie bekommen bei jedem Kauf eine Rechnung auf Ihren Namen mit ausgewiesener MwSt. Alle Angebote auf ebay.de verstehen sich als Brutto. Die Rechnung wird Ihnen mit der Ware zugesandt, auf Wunsch können Sie eine Rechnungs/Kopie vorab als *.PDF per Email zugeschickt bekommen. Rechnungspreis ist der Verkaufspreis der Auktion zuzüglich der Frachtkosten. EBAY Gebühren übernehmen wir. ---------- Garantie: Wir geben auf alle Artikel die bei uns über EBAY gekauft werden eine Garantie von mindestens 12 Monaten, solange es nicht anderes in der Auktion definiert ist. Dazu haben Sie natürlich immer die Garantie des jeweiligen Herstellers. (Oft 12 bis 36 Monate). Im Garantiefall senden Sie uns bitte den Artikel frei mit Fehlerbeschreibung und Rechnungskopie an folgende Adresse zurück: MRW Mediadesign & Distribution - RMA EBAY- Elbestr. 9 49565 Bramsche Nach Eingang und Prüfung der Ware werden wir per Mail mit Ihnen in Kontakt treten. Bei tatsächlichem Defekt der Ware werden wir Ihnen so schnell wie möglich eine Austauschware zuschicken. Sollte der defekte Artikel erst zum Hersteller zur Reperatur oder Austausch eingeschickt werden, kann eine Reklamation ca. 2-6 Wochen dauern. Wir bitten um Ihr Verständniss. Ist ein Artikel, der von Ihnen als Defekt deklariert zu uns eingeschickt wurde, bei uns in der Werkstatt völlig in Ordnung, müssen wir Ihnen eine Techniker Einheit in Höhe von 18,- EUR berechnen. Überprüfen Sie bitte genau, ob der Fehler nicht an Ihren EDV Komponenten liegt. Bei technischen Fragen stehen wir Ihnen auch gerne via E-Mail zur Verfügung. ---------- Gewährleistung: Unvollständige oder unrichtige Lieferungen, sowie

6.2.1 Angebot Neuware, ALTERNATE GmbH, Onlineshop

ALTERNATE™
HARDWARE ▪ SOFTWARE ▪ ENTERTAINMENT

Philipp-Reis-Str. 9
D-35440 Linden (Hess)

24h Bestellhotline 0 180 5 / 90 50 40
(€ 0,14/Min. powered by BTignite)

Acer Aspire T660 Pentium 4 631

Abb. kann vom Original abweichen.

Art.-Nr.: SPEC02

Beschreibung:
Der kompakte schwarz/silberne Acer Aspire T660 macht sowohl auf als auch unter dem Schreibtisch eine gute Figur. Eine 160 GB SATA Festplatte und der DVD-DL-Brenner sorgen für viel Speicherkapazität. Seine Stärke liegt in der Arbeitsgeschwindigkeit, die dank eines Intel® Pentium® 4 631 Prozessors mit 512 MB Arbeitsspeicher und einer 10/100 MBit/s Netzwerkanbindung sehr gut ist. Zudem ist das System Multimadiatauglich über die zahlreichen externen Geräte- und Soundanschlüsse.

€ 489,-*

Weiterführende Informationen

Gehäuse	Gehäusetyp	schwarz/silberner Mini Tower
	5,25 Zoll, extern	2 Schächte
	3,5 Zoll, extern	2 Schächte
	Abmessungen (BxHxT)	180 mm x 360 mm x 420 mm
Prozessor	Bezeichnung	Intel® Pentium® 4 631 (3,0 GHz)
	Kerne	1
	Taktfrequenz	3.000 MHz
Arbeitsspeicher	Gesamtkapazität	512 MB
	Anzahl Module	1
	Typ	SDRAM-DDR
Grafikkarte	Bezeichnung	ATI Radeon Xpress 1100
	Speicher	bis zu 256 MB vom Arbeitsspeicher
	Anschlüsse	VGA
Mainboard	Bezeichnung	ATI RC415 Chipsatz
	Anschlüsse	1x PCIe x16, 1x PCIe x1, 2x PCI, 2x PS/2, Parallel, Seriell, 6x USB 2.0, 1x RJ-45
Netzwerk	10/100 MBit/s	
Optische Laufwerke	16x DVD-DL-Brenner	
Festplatte	160 GB (SATA, 7200 U/min)	
Features	Sound	
Gewicht	11,6 kg	
Software	Microsoft Windows Vista Home Basic, Microsoft Morks	

6.3 Konfigurationsdateien

6.3.1 Konfigurationsdatei des OpenVPN-Servers

baumann.conf

```
local 192.168.82.8
port 1194
proto udp

dev tun

ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
tls-auth /etc/openvpn/keys/ta.key 0
dh /etc/openvpn/keys/dh1024.pem

mode server
server 192.168.92.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/ipp.txt

push "route 192.168.82.0 255.255.255.0"
push "dhcp-option WINS 192.168.82.10"

client-to-client
keepalive 10 30

comp-lzo
max-clients 5

user ovpn
group ovpn

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

status /etc/openvpn/status.log
log /etc/openvpn/server.log

# Set the appropriate level of log
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages in log
mute 20
```

6.3.2 Konfigurationsdatei des OpenVPN-Clients

bmimmoclient.conf

```
client

dev tun

dev-node vnic1

proto udp
remote bmimmo.dyndns.org 1194

resolv-retry infinite

mute-replay-warnings
nobind

ca c:\\programme\\openvpn\\keys\\ca.crt
cert c:\\programme\\openvpn\\keys\\client01.crt
key c:\\programme\\openvpn\\keys\\client01.key
ns-cert-type server
tls-auth c:\\programme\\openvpn\\keys\\ta.key 1

comp-lzo

mute 20
```

© 2007 · Volker Böcker · Bremen

Handelskammer Bremen

Abschlussprüfung: Sommer 2007

im Ausbildungsberuf: Fachinformatiker der Fachrichtung Systemintegration

Prüfungsteilnehmer:	**Ausbildungsbetrieb:**
Volker Böcker	Deutsche Telekom
Prüfungs-Nr.: 7395 erhalten Sie mit der Einladung zur schriftlichen Prüfung	

Projektbezeichnung

Integration eines VPN-Dienstes auf Basis von Transport-Layer-Verschlüsselung

Bestätigung des Ausbildungsbetriebes

Wir bestätigen, dass der/die Auszubildende das oben bezeichnete Projekt einschließlich der Dokumentation im Zeitraum

vom 1.4. bis 18.4. selbständig ausgeführt hat.

Projektverantwortliche/er in Ausbildungsbetrieb

A Pachowsky, 0421/3299-691

Name Telefon Unterschrift

Ausbildungsverantwortliche/er im Ausbildungsbetrieb

Peter Gottwald, 0421 300 5402, i. A.

Name Telefon Unterschrift

Eidesstattliche Erklärung:

Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbständig erstellt und dass ich bei der Erstellung weder vollständig noch teilweise Passagen aus anderen betrieblichen Aufträgen bzw. Dokumentationen übernommen habe, die bei der prüfenden oder einer anderen Kammer eingereicht wurden.

Bremen 16.4.07 Volker Böcker

Ort und Datum Unterschrift des Prüflings

HK HB 01/07

Integration eines VPN-Dienstes

auf Basis von Transport-Layer-Verschlüsselung

Erweiterung eines Intranets zur Bereitstellung einer Fernzugriffsmöglichkeit

Betriebliche Projektarbeit
für die Abschlussprüfung zum
Fachinformatiker für Systemintegration

Volker Böcker | Prüflingsnr. 7395 | 27. Juni 2007
Deutsche Telekom AG | Telekom Training Bremen

Inhalt

1. Einführung
2. Analyse und Planung
3. Kalkulation und Beschaffung
4. Installation und Konfiguration

1.1 Ausbildung und Tätigkeiten

- seit Januar 2005 im ICT-Service tätig
- Closed Area Netzwerk mit ca. 700 PCs und 300 Servern an den Standorten Bremen und Hamburg
- Arbeitsplatz-Service, Server-Betrieb, Servicedesk/Hotline, Netzwerk-Management
- eigene DMZ am Standort Bremen

1.2 Vorstellung des Kunden

- Kleinbetrieb, typischer Familienbetrieb
- Branche: Bauträger und Hausverwaltung
- 6 Beschäftigte
- kleines Intranet mit wenigen essentiellen Diensten
- keine Bindung an einen festen Systemintegrator

Auftragnehmer (fiktiv):

- Bocom GmbH
  Bremer Systemhaus mit 6 Angestellten

2.1 Projektablauf

3 Projektabschnitte für die konkrete Durchführung:

A. Vorbereitung und Planung
- Ist-Zustand sichten
- Leistungsumfang besprechen

B. Beschaffung und Konfiguration
- Anfertigen des Systems
- umfangreiche Vorinstallation

C. Systemintegration vor Ort
- Einbindung des Systems
- Übergabe und Projektabschluss

2.2 Vorhandene Infrastruktur

- 100 Mbit Ethernet, sternförmig, zentraler Technikraum
- Microsoft Windows Domäne, 5 Arbeitsplatz-Rechner, 1 Server und 1 Notebook
- zentraler Fileserver
- gemeinsame Kalender- und Kontakte-Verwaltung
- servergestützte Onlinebanking-Software
- serverbasierte Hausverwaltungs-Software
- Administration durch Teilzeitkraft an Wochenenden

2.3 Anforderungen des Kunden

1. Anbindung des Heimarbeitsplatz-PCs
2. Zugriffsmöglichkeit von unterwegs
3. Fernwartungszugang für die Administratorin
4. Fernzugriffsmöglichkeit für die Sachbearbeiter der Hausverwaltung (optional)

2.4 Das angebotene Konzept

- dedizierter Server als VPN-Gateway mit dem Betriebssystem Linux
- OpenVPN für VPN-Konnektivität auf Layer 3 des OSI-Referenzmodells
- Authentifizierung mittels einer Public-Key-Infrastruktur (Zertifikate)
- Anbindung von 2 Clients an das Intranet, keine Zugriffsbeschränkungen
- WINS-Server für die Namensauflösung

2.5 Begründung und Alternativen

- sehr gute Erfahrungen mit dem System
- geringe Hardware-Voraussetzungen (Standard-PC)
- gute Skalierbarkeit und einfache Wartung
- keine Lizenzkosten
- Linux als gute Plattform für optionale Dienste
- Alternativen: Microsoft Windows Server
  Draytek Vigor xDSL-Router-Serie
  T-Com T-Online directVPN

3.1 Benötigte Hard- und Software

- Server-Hardware

  Prozessor: Intel x86-Plattform, ab 450 MHz,
  Arbeitsspeicher: 128 MB, Festplattenspeicher: 15 GB
  Netzwerkkarte: 100BaseTX Ethernet, RJ45-Anschluss,
  CD-ROM-Laufwerk, Diskettenlaufwerk

- Software

  Ubuntu Linux 6.06 LTS Server
  OpenVPN 2.0.9 (enthält OpenSSL-Suite)

3.2 Auswahlkriterien für den Server

Hohe Priorität:

- möglichst gute Dimensionierung
- geringe Anschaffungskosten
- geringer Energieverbrauch

Niedrige Priorität:

- hohe Leistungsreserven
- Hochverfügbarkeit
- Hersteller-Support

3.3 Angebote im Vergleich

Gebraucht-PC, eBay-Händler	Neuware, ALTERNATE GmbH
Fujitsu Siemens Scenic D i815e	**Acer Aspire T660**
MiniDesktop, ATX Intel Pentium III, 1,0 GHz 256 MB SD-RAM, 40 GB HDD DVD-ROM, Floppy, Ethernet-Karte	Minitower, ATX Intel Pentium IV, 3,0 GHz 512 MB DDR-SDRAM, 160 GB HDD DVD-DL-RW, Ethernet-Karte
Preis: EUR 85,00 inkl. MwSt. **+ Versandkosten EUR 13,50** **= EUR 98,50**	**Preis: EUR 489,00 inkl. MwSt.** **+ Versandkosten EUR 12,00** **= EUR 501,00**

3.4 Die Internetanbindungen

- möglichst hohe Upstream-Bandbreite am Serverstandort
- ADSL2+-Anschluss verfügbar (16/1 Mbit)
- Limitierung durch effektive Datendurchsatzrate des Internets
- VPN-Nutzer sensibilisieren

3.5 Tabellarische Kostenkalkulation

		Einzelpreis	Gesamtpreis
Materialkosten			
1 x	Gebraucht-PC FSC Scenic L i815 (eBay-Händler)	85,00 €	85,00 €
1 x	Versandkosten Lieferant	13,50 €	13,50 €
1 x	Netzwerkkabel CAT5 STP, 10 m	7,50 €	7,50 €
Summe Materialkosten			106,00 €
Fertigungskosten			
26 x	Arbeitslohn Bocom GmbH IT-Azubi	45,00 €	1.170,00 €
2 x	Fahrtkosten-Pauschale Regionalbereich	30,00 €	60,00 €
Summe Fertigungskosten			1.230,00 €
Summe Herstellkosten = Material- + Fertigungskoten			**1.336,00 €**
Zuschlag Verwaltungsgemeinkosten (10 %)			+ 133,60 €
Zuschlag Vertriebsgemeinkosten (10 %)			+ 133,60 €
Summe Selbstkosten			**1.603,20 €**
Gewinnzuschlag (10 %)			+ 160,32 €
Gesamtpreis netto			1.763,52 €
Umsatzsteuer (19 %)			335,07 €
Gesamtpreis brutto			**2.098,59 €**

4.1 Phase I: Vorinstallation

VPN-Server Grundsystem

- Ubuntu Linux Server Basis-Installation
- aktuelles OpenVPN Release als Dienst

OpenVPN Server-Konfiguration

- ein einziger offener Port nach außen (1194/udp)
- eigenes Subnetz 192.168.92.0/24
- die Clients erhalten eine Route ins Intranet
- und die Adresse des WINS-Servers via „push“

4.2 TLS und PKI

Transport-Layer-Security-Protokoll (TLS)

- arbeitet zwischen der Transportschicht (Layer 4) und den Anwendungsschichten

Public-Key-Infrastruktur (PKI)

- asymmetrisches Verfahren
- eigene Zertifizierungsstelle

„easy-rsa“

- Skripte zur komfortablen Bedienung von OpenSSL

4.3 Phase II: Integration vor Ort [1/2]

VPN-Server

- Aufstellen des Servers im Technikraum
- Anpassen der Netzwerkeinstellungen

Konfiguration des Intranets

- WINS-Dienst installieren
- statische IP-Adressen und WINS-Server eintragen
- statische Route im Gateway setzen
- Port öffnen, DynDNS-Dienst einrichten

4.3 Phase II: Integration vor Ort [2/2]

VPN-Clients

- Download und Installation
- Kopieren der Konfigurationsdatei
- Personal Firewall beachten
- Dienst automatisch starten

Funktionstest

- Routing und Konnektivität mittels ICMP-Tool „ping“
- Keep-Alive-Funktion wichtig für Bedienungskomfort

4.4 Projektabschluss

Übergabe des Systems

- Zusammenfassung
- Hinweis auf fehlende Ausfallsicherheit
- und systembedingte Limitierungen
- Empfehlungen für die Fernwartung

Feedback des Kunden

- nach Testphase sehr zufrieden mit dem VPN
- Fernadministration unkompliziert und effizient

Vielen Dank für Ihre Aufmerksamkeit.