Projektdokumentation

Planung und Integration
einer Firewall-Lösung

von
Florian Baumann
Berufsschule 1, ITK12a
Bayreuth
florian.baumann@tmt.de

Ausbildungsbetrieb:
TMT Teleservice GmbH & Co. KG
Nürnbergerstraße 42
95448 Bayreuth
tech@tmt.de

Inhaltsverzeichnis

1. Projektumfeld

1.1 Firmenvorstellung

Die Firma „TMT TeleService GmbH & Co.KG“ (im weiteren Verlauf „TMT“) in Bayreuth, deckt 3 wichtige Bereiche moderner Kommunikation ab. TMT bietet somit eine abgestimmte und ganzheitliche Produktpalette in den Bereichen „Webdevelopment und Design“, „Call Center“ und „IT- und Netzwerk-Sicherheit“. Derzeit sind etwa 50 Mitarbeiter beschäftigt.

Aufgabe der Abteilung „IT- und Netzwerk-Sicherheit“, der ich während diesem Projekt angehörte, ist die Pflege der mittlerweile mehr als 200 Server (95% davon mit der Betriebssystembasis Linux) und Realisierung von netzwerkbezogenen Kundenaufträgen sowie Einrichtung und Betreuung der hauseigenen Produktlinie TMT-blueHost.

1.2 Beschreibung des Umfeldes

Die Firma „Logistika GmbH“ (nachfolgend „Logistika“) ist ein mittelständisches Unternehmen im Bereich Logistik. Aus wirtschaftlichen sowie geographischen Gründen ist Logistika im Begriff den Firmensitz an einen anderen Standort umzuziehen und beauftragt TMT mit der Konzeption des neuen hausinternen Netzwerks und der Anbindung ins Internet.

2. Projektdefinition

Bei der firmeninternen Ausarbeitung des Konzepts fiel mir die Planung und Einrichtung der Firewall-Lösung zu. Somit wurde es zu meiner Aufgabe ein geeignetes Gerät, Betriebssystem und eine Firewall-Software auszuwählen. Desweiteren lag ein Schwerpunkt auf genauer Konfiguration der benötigten Portfreigaben, sowie Einrichtung der von Logistika gewünschten VPN-Zugänge, um das Arbeiten von Außendienstmitarbeitern zu erleichtern. Alles in allem sind ca. 80 Desktop-PCs und 3 Server am neuen Standort von Logistika vorhanden.

Projektziel war es, innerhalb einer Woche die ausgearbeitete Firewall-Lösung vollkommen funktionstüchtig in die Netzwerk-Infrastruktur zu integrieren.

3. Ist-Analyse

Aufgrund des Umzuges und der Neueinrichtung des EDV-Systems waren nur sehr wenige Systemkomponenten vorhanden. Der neue Standort der Logistika GmbH wurde bereits im Vorfeld von einem Elektro-Installateur Unternehmen mit den nötigen Patchfeldern versehen. (Infrastrukturplan Logistika, Anhang 8.1)

Vorhandene Komponenten		Ist-Analyse
Netzwerk	System	Ethernet 100BaseTX
	Topologie	Stern
	Verkabelung	UTP CAT5
	Switches	4 Netgear GSM7352S

Wegen des veralteten Zustandes der vorherigen Firewall, musste auch neue Hardware für die Firewall bezogen werden. Diese ist zusätzlich Bestandteil des Angebots.

4. Soll-Konzept

4.1 Anforderungen Logistika (Kunde)

Innerhalb einer Woche soll, wie mit Logistika vereinbart, die Firewall-Lösung in das Netzwerk integriert (wie im Infrastrukturplan, Anhang 8.1 ersichtlich) und einsatzbereit sein. Logistika stellte außerdem folgende Anforderungen an die Firewall:

- Interne Erreichbarkeit der Firewall via SSH
- Verbindung ins WAN für Arbeitsplätze
- Garantierte Weiterleitung und Erreichbarkeit des internen Mailservers
- VPN-Verbindungen ins interne Netz

4.2 Anforderungen TMT (Dienstleister)

Weitere Anforderungen an die Firewall, um die Wartung und Pflege des EDV-Systems von Logistika zu erleichtern:

- Remote-Verbindungen zu internen Windows-Servern muss bestehen
- Erreichbarkeit des FileServers mit dem Cacti-Monitoring-System
- Firewall darf, aus Sicherheitsgründen, extern via SSH nur von TMT erreichbar sein

4.3 Hardware der Firewall

Aufgrund des veralteten Zustands der Firewall suchte ich mir ein für Firewalls geeignetes Modell, aus dem Bestand von TMT, als neue Basis für die Firewall-Lösung:

Benötigte Komponenten		Ist-Analyse
Server	Typ	Nexgate NSA 1030-R
	Größe	19 Zoll, 1HE
	Prozessor	VIA 800MHz
	Festplatte	40 GB
	Arbeitsspeicher	512MB
	Netzwerkkarten	100Mbit/s (Intern, Extern, DMZ)

4.4 Software der Firewall

Die Software, die später einmal die Interaktionen zwischen privatem Netz und Internet kontrolliert, war mit Bedacht zu wählen. Aufgrund guter eigener Erfahrungen mit der Firewall-Software „Shorewall“ wurde diese, nach Rücksprache mit Kollegen, von mir ausgewählt. Außerdem benötigte ich ein Programm zur Fernwartung der Firewall und die nötigen Pakete zur Verbindung der Außendienstmitarbeiter über VPN. Bei der Fernwartung entschied ich mich für SecureShell (SSH), da dies der Standard unter Linux ist und bei so gut wie allen Servern von TMT eingerichtet ist. Aus Gründen der Kompatibilität mit Windows und der einfachen Handhabung, wählte ich das Programm `pptpd` für die VPN-Verbindung.

Benötigte Komponenten		Ist-Analyse
Software	Betriebssystem	debian-etch-40r6_i386
	Programme Firewall	shorewall-3.2.6-2_all.deb
		iproute_20061002_i368.deb
	Programme Fernwartung	openssh-server_4.3p2-9etch3_i386.deb
	Programme VPN	ppp_2.4.4rel-8_i386.deb
		pptpd_1.3.0-2etch2_i386.deb

5. Planung der Projektschritte

5.1 Struktur- und Zeitplanung

Die nachfolgende Gliederung gibt eine kurze Übersicht über die wichtigsten Projektschritte und deren zeitlichen Ablauf:

1.	Analyse des IST-Zustandes	3 Std.
2.	Ausarbeitung des Soll-Konzepts	3 Std.
3.	Erstellung des Angebots	2 Std.
4.	Vorbereitung der Hardware	2 Std.
5.	Installation des Grundsystems	2 Std.
6.	Einrichtung Fernwartung	2 Std.
7.	Einrichtung der Firewall	9 Std.
8.	Einrichtung der VPN-Verbindung	5 Std.
9.	Integration und Inbetriebnahme des Servers	4 Std.
10.	Test des Systems	3 Std.
Gesamt		35 Std.

5.2 Kosten- / Nutzenanalyse

Hauptkriterium für die Auswahl der Systemkomponenten war der Preis. Wie genau sich die Kosteneinsparungen der OpenSource-Lösung auswirken, wird in der nachfolgenden Tabelle anschaulich gemacht. (Netto inkl. Aufschläge)

	Debian-Linux 4.0	Windows Server 2008	GateProtect GPA250
geeigneter Server	654,00 €	1020,00 €	1666,00 €
Betriebssystem	-	695,00 €	inklusive
Firewall/VPN Software	-	inklusive	inklusive
Dienstleistung (25 Std.)	1875,00 €	1875,00 €	1875,00 €
Gesamt	**2529,00 €**	**3590,00 €**	**3541,00 €**

Aufgrund der OpenSource-Lösung fallen bis auf Dienstleistung und Hardware keine weiteren Kosten an. Aus Kulanzgründen werden IST-Analyse, Soll-Zustand, Erstellung des Angebots und Vorbereitung der Hardware nicht berechnet (Angebot im Anhang 8.4).

6. Projektrealisierung

6.1 Hardware

Nachdem das erstellte Angebot unverzüglich von Logistika angenommen wurde, wählte ich aus Beständen von TMT einen Nexgate NSA 1030-R. Dieser Server bot passend zum geplanten Linux Betriebssystem, die entsprechende Hardware. Nachdem die Tauglichkeit der Hardware festgestellt war, schloss ich den Server an die Testumgebung der Werkstatt von TMT an. Um die Installation des Debian Systems durchzuführen waren allerdings einige Vorkehrungen nötig. Die Hardware verfügt standardmäßig über keinen USB-, VGA- und

PS2-Anschluss. Ein CD-ROM-Laufwerk ist ebenfalls nicht vorhanden. Entsprechende Hardware wurde an dem Mainboard angebracht.

6.2 Grundkonfigurationen

Folglich konnte ich das Debian-Linux-Image „debian-etch-40r6_i386“ aus dem Verzeichnis `http://cdimage.debian.org/debian-cd/4.0_r6/i386/iso-cd/` herunterladen, auf CD brennen und installieren. Die Partitionierung der zukünftigen Firewall wählte ich wie folgt:

```
/boot          - 0,05 GB
Swap           - 1 GB
/              - 39 GB
```

Nach erfolgreicher Installation des Debian Grundsystems richtete ich die Bezugsquellen für Debian-Pakete in `/etc/apt/sources.list` ein:

```
deb ftp://mirror.tmt.de/debian etch main non-free contrib
deb-src ftp://mirror.tmt.de/debian etch main non-free contrib
```

Diese Quellen wurden aus Geschwindikeits- sowie Stabilitätsgründen auf die TMT eigenen Spiegelserver umgestellt. Um das Arbeiten von meinem Arbeitsplatz aus zu erlauben, sowie die spätere Fernwartung der Firewall zu stellen, installierte ich `openssh-server`. Anschließend kontrollierte ich die Konfiguration in `/etc/ssh/sshd_config` und deaktivierte, aus Sicherheitsgründen, durch hinzufügen von `PermitRootLogin no`, den Root-Login. So konnten meine späteren Arbeiten am Arbeitsplatz ausgeführt werden. Da die zusätzlich angebrachten Komponenten nun nicht mehr gebraucht wurden, entfernte ich diese wieder. Den eingebauten VGA-Adapter beließ ich an seinem Platz, da er am Gehäuse befestigt werden konnte und eventuell später erneut von Nutzen ist.

6.3 Firewall

Nun war die Einrichtung der Firewall-Software „Shorewall“ an der Reihe. Wie gewohnt installierte ich mit „`apt-get install shorewall`“ die Software. Steuerungs- und Konfigurationsdateien von Shorewall mussten in `/etc/shorewall/` erstellt werden. Um dem Benutzer einen Schritt weit entgegen zu kommen, liegen in dem Verzeichnis `/usr/share/doc/shorewall/` einige Dateien, die als Orientierungshilfe verwendet werden können. Es wurden: `hosts`, `interfaces`, `masq`, `policy`, `rules`, `tunnels` und `zones` benötigt und somit in das entsprechende Verzeichnis kopiert. Um der Firewall erst einmal Struktur zu verleihen, begann ich mit der Definition der Zonen. Zonen stellen grundsätzliche Bereiche des Firewall-Systems dar.

```
zones:  ZONE    TYPE            OPTIONS         IN      OUT
        fw      firewall
        net     ipv4
        loc     ipv4
        pptp1   ipv4            #VPN
```

Die definierten Zonen spielen eine wesentliche Rolle, da diese später in jeder anderen Datei als Aliase verwendet werden können. Sowie in der `interfaces`-Datei, die wie folgt angelegt wurde:

```
interface:      ZONE    INTERFACE       BROADCAST       OPTIONS
                net     pppoe0          detect          norfc1918,tcpflags,nosmurfs
                loc     eth1            detect          tcpflags,nosmurfs
                pptp1   ppp+            detect          nosmurfs,tcpflags       #VPN
```

In `interfaces` werden also Netzwerkkarten mit Funktionen bzw. Protokollen belegt. Als nächstes Regelwerk steht die Editierung der Datei `policy` an, die die allgemeinen Rechte der Zonen untereinander festlegt .

```
policy:         SOURCE          DEST    POLICY          LOGLEVEL        LIMIT:BURST
                fw              all     ACCEPT
                loc             net     ACCEPT
                pptp1           loc     ACCEPT          #VPN Extern->Intern
                loc             pptp1   ACCEPT          #VPN Intern->Extern
                loc             fw      ACCEPT
                all             all     REJECT
```

Um trotzdem die Funktion spezieller Dienste zu gewährleisten, mussten Detail-Freigaben konfiguriert werden. Die anspruchsvollste Datei des Projekts war am besten aus den Anforderungen von Logistika und TMT abzuleiten. Hier dürfen keinerlei Fehler oder unnötige Regeln definiert sein, da sonst die Sicherheit/Funktionstüchtigkeit des gesamten internen Netzes auf dem Spiel steht. (Öffentliche IP-Adressen aus Sicherheitsgründen abgeändert)

```
rules:  ACTION  SOURCE                  DEST            PROTO   DESTPORT        ORGINGALDEST
        #Interne Freigaben
        ACCEPT  loc                     fw              tcp     22                              #SSH intern
        ACCEPT  loc                     fw              upd     53                              #DNS intern
        #TMT Freigaben
        ACCEPT  net:181.145.98.130,181.145.98.153       fw      tcp     22      #SSH FW-TMT,Nagios
        ACCEPT  net:181.145.98.130,181.145.98.153       fw      icmp            #SSH FW-TMT,Nagios
        #Exchange Weiterleitungen (DNATs sind Weiterleitungen zu internen Servern)
        DNAT    net             loc:172.16.0.10         tcp     25              #IMAP Mailserver
        DNAT    net             loc:172.16.0.10         tcp     80              #WebAccess Mail
        DNAT    net             loc:172.16.0.10         tcp     443             #WebAccess Mail
        #RDP Weiterleitung Interne Server
        DNAT    net:181.145.98.130      loc:172.16.0.10:3389    tcp     9595    #Remote FileServer
        DNAT    net:181.145.98.130      loc:172.16.0.11:3389    tcp     9596    #Remote OracleServer
        DNAT    net:181.145.98.130      loc:172.16.0.12:3389    tcp     9597    #Remote PostServer
        #Monitoring-System Cacti Zugriff auf FileServer
        DNAT    net:181.145.98.130      loc:172.16.0.10:161     udp     1161    #Cacti SNMP
```

Diese Regeln gewährleisten optimalen Schutz des internen Netzes ohne Einbußen in der Pflege oder Nutzung machen zu müssen. Die Firewall ist somit also funktionstüchtig.

Weiterhin sind alle bearbeiteten Konfigurationsdateien von `shorewall` noch einmal vollständig im Anhang aufgelistet.

6.4 VPN

Um die Außendienstmitarbeiter auch von außerhalb ins Unternehmens-Netzwerk zu integrieren, ist eine VPN-Verbindung notwendig. Dazu muss auf der Firewall (die sozusagen die Tür von Logistika darstellt) eine entsprechende Software installiert sein, die die Benutzer durch die Tür ins interne Netz weiterleitet. Die Software die sozusagen den Türsteher spielt ist `pptpd`. Zusätzlich wird `ppp` benötigt, das als Protokoll für die VPN-Verbindung agiert.

```
apt-get install ppp pptpd
```

Zunächst einmal wurde grundsätzlich `pptp` konfiguriert und einige Einträge in `/etc/pptpd.conf` angepasst. Darunter die IP des VPN-Servers, Unterdrückung der Client-IP-Adressen und den IP-Pool für VPN Benutzer.

Auch in der Firewall müssen aufgrund des VPN-Zuganges noch weitere Einstellungen angepasst werden. Um die VPN-Clients einer Zone zuzuweisen, wird die Datei `hosts` (IP-Pool) und für die Existenz des VPN-Systems `tunnels` editiert. (Firewall-Files, Anhang 8.2.1)

Nachdem die Benutzerdaten, die später die Außendienst-Mitarbeiter erhalten, in `ppp` registriert waren (`ppp - /etc/ppp/chap-secrets`, Anhang 8.2.2), stand eine weitere Anpassung von `ppp` an. pptpd-options wird von der Protokoll-Config (pptpd.conf) nachgeladen und beinhaltet diverse Einstellungen zur Kompatibilität.

```
ms-dns 172.16.0.10          #Windows DNS FileServer
ms-wins 172.16.0.10         #Kompatibilität für Windows Clients
debug                       #Schaltet debugging an in /var/log/syslog
```

6.5 Integration und Test des Systems

Logistika ist via DSL-Einwahl-Modem mit dem Internet verbunden. Um Verbindung mit dem WAN herzustellen müssen also Benutzerdaten an das Modem übergeben werden. Diese werden in `dsl-provider` (`/etc/ppp/peers/dsl-provider`, Anhang 8.2.2) definiert.

Folglich unterstützt die Firewall auch die Übertragung der Logindaten für die DSL-Anbindung und ist damit einsatzbereit. Die Integration in das mittlerweile bestehende Netzwerk benötigte weniger Aufwand. Lediglich durch zwei Patchkabel (Intern/Extern) an eth0 und eth1 band ich die Firewall in die Infrastruktur ein. Außerdem konfigurierte ich die beiden Interfaces der Netzwerkkarten dem Standort gerecht, in `/etc/network/interfaces` um (Anhang 8.2.3). Nach problemfreien Start aller Anwendungen am Endstandpunkt, befand ich

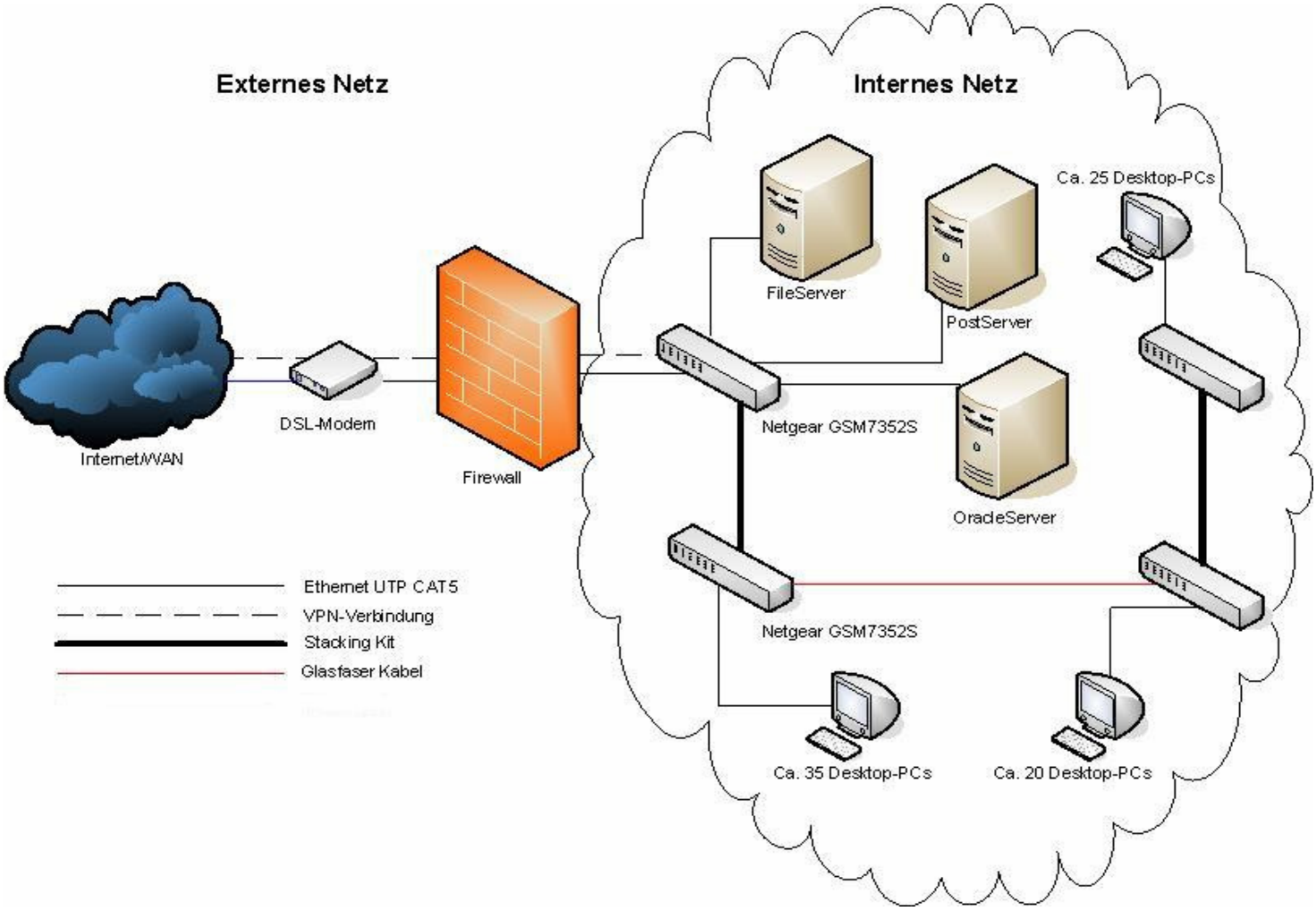
die Firewall-Lösung für funktionstüchtig. In Absprache mit Kollegen prüften wir (über Telefon in Kontakt) verschiedene Regeln der Firewall und die VPN-Einwahl. Anschließend vergab ich die VPN Logindaten an die Mitarbeiter des Außendienstes und richtete an deren Laptops die Verbindungen ein.

7. Schlussbetrachtung

Das von mir, im Rahmen meiner betrieblichen Ausbildung bei der TMT-Teleservice GmbH & Co.KG, durchgeführte Projekt konnte erfolgreich abgeschlossen werden. Die Firewall-Lösung verrichtet seither ihre Dienste für die Logistika GmbH und weist (abgesehen von Heimarbeitsplatz bedingten Verbindungsproblemen der Außendienst Mitarbeiter) keinerlei Probleme auf. Im weiteren Verlauf wurde eine weitere Freigabe für einen zusätzlichen Server Logistikas eingetragen. Was sich aber dank einfacher Handhabung von `shorewall` und routiniertem Umgang leicht umsetzen ließ. Insgesamt wurde der Zeitrahmen eingehalten.

8. Anhänge

8.1 Netzwerk-Infrastruktur



8.2 Erstellte Konfigurationsdateien

Komplette Darstellung der in der Projektarbeit verwendeten / erstellten Konfigurationsdateien. Der Übersichtlichkeit wegen ohne Kommentare, Erklärungen und Beispielen.

8.2.1 Firewall

```
# Shorewall version 4 - Zones File
#ZONE   TYPE            OPTIONS         IN                      OUT
#                                       OPTIONS                 OPTIONS
fw      firewall
net     ipv4
loc     ipv4
pptp1   ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

```
# Shorewall version 4 - Interfaces File
#ZONE   INTERFACE      BROADCAST      OPTIONS
net     pppoe0         detect         norfc1918,tcpflags,nosmurfs
loc     eth1           detect         tcpflags,nosmurfs
pptp1   ppp+           detect         nosmurfs,tcpflags
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

```
# Shorewall version 4 - Policy File
#SOURCE         DEST           POLICY         LOG            LIMIT:BURST
fw              all            ACCEPT
loc             net            ACCEPT
pptp1           loc            ACCEPT
loc             pptp1          ACCEPT
loc             fw             ACCEPT
all             all            REJECT
#LAST LINE -- DO NOT REMOVE
```

```
# Shorewall version 4 - Rules File
#ACTION         SOURCE         DEST           PROTO   DEST    SOURCE         ORIGINAL       RATE
#                              PORT                           PORT(S)        DEST           LIMIT
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
ACCEPT          loc                           fw              tcp     22
ACCEPT          loc                           fw              udp     53
ACCEPT          net:181.145.98.130,181.145.98.153   fw        tcp     22
ACCEPT          net:181.145.98.130,181.145.98.153   fw        icmp
DNAT            net                           loc:172.16.0.10       tcp     25
DNAT            net                           loc:172.16.0.10       tcp     80
DNAT            net                           loc:172.16.0.10       tcp     443
#RDP zum Fileserver / Exchange
DNAT            net:181.145.98.130            loc:172.16.0.10:3389  tcp     9595
#RDP zum OracleServer
DNAT            net:181.145.98.130            loc:172.16.0.11:3389  tcp     9596
#RDP zum PostServer
DNAT            net:181.145.98.130            loc:172.16.0.12:3389  tcp     9597
#Cacti SNMP
DNAT            net:181.145.96.110            loc:172.16.0.10:161   udp     1161
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

```
# Shorewall version 4 - Hosts file
#ZONE   HOST(S)                               OPTIONS
pptp1   ppp+:172.16.0.200-172.16.0.209            tcpflags,nosmurfs
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS LINE -- DO NOT REMOVE
```

```
# Shorewall version 4 - Masq file
#INTERFACE              SOURCE          ADDRESS         PROTO   PORT(S) IPSEC   MARK
pppoe0                  eth1
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

```
# Shorewall version 4 - Tunnels File
#TYPE                   ZONE    GATEWAY         GATEWAY
#                                               ZONE
pptpserver                net     0.0.0.0/0
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

8.2.2 VPN

```
# pptpd - /etc/pptpd.conf
option /etc/ppp/pptpd-options
debug
noipparam
#logwtmp
#bcrelay eth1
localip 172.16.0.1
remoteip 172.16.0.200-209
```

```
# ppp - /etc/ppp/pptpd-options
name pptpd
#chapms-strip-domain
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
mppe required,stateless,no40,no56
ms-dns 172.16.0.10
#ms-dns 10.0.0.2
ms-wins 172.16.0.10
#ms-wins 10.0.0.4
proxyarp
nodefaultroute
debug
#dump
lock
nobsdcomp
```

```
# ppp - /etc/ppp/chap-secrets
# client              server          secret                  IP addresses
"Mitarbeiter1"        *               "Passwort1"             *
"Mitarbeiter2"        *               "Passwort2"             *
"Mitarbeiter3"        *               "Passwort3"             *
```

```
# ppp - /etc/ppp/peers/dsl-provider
plugin userpass.so
ifname pppoe%d
noipdefault
noproxyarp
noipx
noipv6
defaultroute
replacedefaultroute
hide-password
lcp-echo-interval 15
lcp-echo-failure 3
noauth
persist
maxfail 0
holdoff 5
# mtu 1492
usepeerdns
linkname dsl-provider
logfile /var/log/dsl-provider.log
# alternative to rp-pppoe.so
# pty "/usr/sbin/pppoe -I ethX -T 80 -m 1452 -U"
plugin rp-pppoe.so eth0
user "telekomusername"
password "telekompasswort"
```

8.2.3 Netzwerk

```
# network - /etc/network/interfaces

auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
        address 172.16.0.1
        netmask 255.255.0.0
        network 172.16.0.0
        broadcast 172.16.255.255

auto dsl-provider
iface dsl-provider inet ppp
        provider dsl-provider
        pre-up /sbin/ifconfig eth0 up # line maintained by pppoeconf
        pre-up /usr/sbin/ppp-watchdog start pppoe0 2 # line maintained by pppoeconf
        post-down /usr/sbin/ppp-watchdog stop pppoe0 2 # line maintained by pppoeconf
        post-down /sbin/ifconfig eth0 down # line maintained by pppoecon


# network - /etc/resolv.conf
search logistika.de
nameserver 172.16.0.10
nameserver 181.145.99.9
```

8.3 Server Details

Server		Ist-Analyse
FileServer	Betriebssystem	Windows Server 2008
	Aufgaben	Fileserver, Exchange, DNS, DHCP
OracleServer	Betriebsystem	Windows Server 2008
	Aufgaben	Datenbank Server Logistik
PostServer	Betriebssystem	Windows Server 2008
	Aufgaben	Adressdatenbank

8.4 Angebot

Angebot auf der Folgeseite