# Dokumentation M146

Internetanbindung für ein Unternehmen realisieren

2009-05-18

Emanuel Duss

# Über

| | |
|---|---|
| Autor | Emanuel Duss |
| Erstellt | 2009-03-02 |
| Bearbeitet | 2009-05-18 |
| Heute | 2011-11-28 |
| Bearbeitungszeit | 12:33:34 |
| Lehrjahr des Moduls | 3. Lehrjahr 2008 / 2009 |
| Pfad | / mnt/Schule/3_Lehrjahr/146_Internetanbindung_fuer_ein_Unternehmen_realisieren/M146_Dokumentation.odt |
| CC-Lizenz |  Creative Commons Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 2.5 Schweiz http://creativecommons.org/licenses/by-nc-sa/2.5/ch/ |
| Powered by |  |

# Bearbeitungsprotokoll

| Datum | Änderung(en) |
|---|---|
| 2009-03-02 | Erstellt |

# Inhaltsverzeichnis

# Modulbaukasten



## Modulidentifikation

| | | |
|---|---|---|
| Modulnummer | 146 | |
| Titel | Internetanbindung für ein Unternehmen realisieren | |
| | | |
| Kompetenz | Entwickeln, Planen und Realisieren von Internetanschlüssen für Unternehmen unter der Berücksichtigung von Sicherheits-, Verfügbarkeits- und Leistungsaspekten. | |
| | | |
| Handlungsziele | 1. | Analysieren des Bedarfs, der Sicherheitsvorgaben und der Verfügbarkeitsanforderungen an einen Internetanschluss. |
| | 2. | Klassieren der eruierten Anforderungen nach Prioritäten und Bedeutung für das Unternehmen und erstellen eines Pflichtenheftes für die Evaluation eines Serviceproviders. |
| | 3. | Resultate der Evaluation unter Berücksichtigung des Pflichtenheftes und wirtschaftlichen Aspekten bewerten und Entscheid herbeiführen. |
| | 4. | Entwickeln und dokumentieren des Designs für den Internetanschluss. Dabei unter Berücksichtigung der Anforderungen Firewall-, DMZ-, Proxy- und DNS-Aspekte berücksichtigen. |
| | 5. | Erforderliche Hardware- und Softwarekomponenten bestimmen und Beschaffungsantrag erstellen. |
| | 6. | Inbetriebnahme der Internetanbindung mit ihren Komponenten planen und realisieren. Abnahme organisieren und durchführen. |
| | 7. | Entwickeln und dokumentieren von Prozessen zur Überwachung der Sicherheit und für den Betrieb der Systeme. |
| | | |
| Kompetenzfeld | Network Management | |
| Objekt | Bestehendes Client/Server Netzwerk und neuer ISP Anschluss. | |
| Niveau | 3 | |
| Voraussetzungen | • Kenntnisse der wichtigsten Sicherheitsanforderungen im Bereich Internet<br>• Kenntnisse der Techniken zur Anbindung von lokalen Netzwerken ans Internet<br>• Erfahrung im Aufbau von lokalen Netzwerken | |
| Anzahl Lektionen | 40 | |
| Anerkennung | Eidg. Fähigkeitszeugnis Informatiker/Informatikerin | |
| | | |
| Modulversion | 1.1 | |
| MBK Release | R3 | |
| Harmonisiert am | 19.09.2006 | |
| | | |

## Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissenselemente, die das Erreichen einzelner Handlungsziele eines Moduls unterstützen. Die Beschreibung dient zur Orientierung und hat empfehlenden Charakter. Die Konkretisierung der Lernziele und des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

| | |
|---|---|
| Modulnummer | 146 |
| Titel | Internetanbindung für ein Unternehmen realisieren |
| Kompetenzfeld | Network Management |
| Modulversion | 1.1 |
| MBK Release | R3 |

| Handlungsziel | Handlungsnotwendige Kenntnisse | |
|---|---|---|
| 1. | 1. | Kennt die wichtigsten Kategorien von Anforderungen (Bandbreite, Verfügbarkeit, Supportumfang, Sicherheit etc.) an eine Internetanbindung und kann für typische Anwenderprofile die üblichen Leistungsmerkmale nennen. |
| 2. | 1. | Kennt die prinzipiellen technologischen Zugangsmöglichkeiten zum Internet sowie deren Anbieter (Provider) und kann die notwendigen infrastrukturellen Voraussetzungen aufzeigen. |
| | 2. | Kennt die wichtigsten Abschnitte eines Pflichtenhefts und kann aufzeigen, was bei der Ausarbeitung dieser Abschnitte hinsichtlich der Erstellung und Beurteilung von Offerten beachtet werden muss. |
| 3. | 1. | Kennt die wichtigsten Kriterien bei der Auswahl eines Angebotes und kann aufzeigen, welche Abhängigkeiten zwischen diesen Kriterien für den Entscheid zu beachten sind. |
| 4. | 1. | Kennt die Komponenten für den Anschluss eines LAN an das Internet (Router, WAN Anschluss, Names- und Nummerierungsschema) und kann aufzeigen, wie diese den Zugang ermöglichen und regeln. |
| | 2. | Kennt die Regeln für das Erstellen eines Namens- und Nummerierungskonzepts und kann erläutern, welchem Zweck Namen und Nummern zur Sicherstellung des Kommunikationsbetriebs in einem Netzwerk dienen. |
| | 3. | Kennt den Funktionsumfang eines Proxy und eines Firewalls und kann aufzeigen, welche Anforderungen hinsichtlich Sicherheit sowie Zugang ins Internet sich damit umsetzen lassen. |
| 5. | 1. | Kennt die wichtigsten Informationen, welche eine Beschaffungsempfehlung beinhalten muss und kann aufzeigen, welche Regeln dabei für eine verständliche und nachvollziehbare Empfehlung zu beachten sind. |
| 6. | 1. | Kennt die Vorgehensweise bei der Planung und Inbetriebnahme eines Internet¬zugangs und kann für die einzelnen Schritte aufzeigen, welchen Beitrag diese zu einer erfolgreichen Inbetriebnahme und zu einem gesicherten Betrieb leisten. |
| | 2. | Kennt Aspekte, die bei der Übergabe eines Systems in den operativen Betrieb beachtet werden müssen und kann den Beitrag der erforderlichen Schritte zur Qualität der Abnahme darlegen. |
| 7. | 1. | Kennt die wichtigsten Sicherheits- und Überwachungsmassnahmen beim Betrieb eines Internetanschlusses und kann erläutern, wie diese eingesetzt werden und wie sie zum Eliminieren und Erkennen der häufigsten Gefahren bei der Nutzung des Internets beitragen. |

# 1 Grundlagenbeschaffung

## 1.1 Hacker & Co

Der Begriff „Hacker“ ist sehr umstritten und nirgends genau definiert. Die meisten Menschen bringen den Begriff sofort mit etwas negativem in Verbindung. Auch in der Presse wird ein Hacker eher schlecht dargestellt.

### Hacker

Das Wort wird umgangssprachlich gebraucht, um jemand zu bezeichnen, der über ein Netzwerk in Computersysteme eindringt und zugleich Teil einer entsprechenden Subkultur ist.[1]

Es gibt viele Definitionen, welche hauptsächlich etwas mit technischem Können, einer Freude an der Lösung von Problemen und dem Übertreten von Grenzen zu tun haben. Hacker lösen Probleme und bauen Dinge auf, sie glauben an Freiheit und freiwillige, gegenseitige Hilfe.[2]

Hacker sind also die „guten“.

### Haecksen

Haecksen sind weibliche Hacker.

### Cracker

"Böse" Hacker heissen Cracker. Diese Leute verstehen ihr Handwerk genau wie die Hacker. Allerdings dringen sie in fremde Systeme ein, um dort Schaden anzurichten. Sie löschen, verändern oder missbrauchen geschützte Datenbestände oder Programme. Durch solche Eingriffe können materielle Schäden in Millionenhöhe entstehen. [3]

Der grundlegende Unterschied ist: Hacker bauen Dinge auf, Cracker zerstören sie.[4]

### Script-Kiddie

Und dann gibt es da noch die so genannten Script Kiddies. Die heissen Kiddies, weil es sich meistens um Jugendliche handelt. Script Kiddies wissen meist überhaupt nicht, was sie tun – halten sich selbst aber für Hacker. Im Gegensatz zu diesen verwenden sie jedoch ausschliessliche vorgefertigte Computerprogramme, z. B. Computerviren oder Trojanische Pferde.[5]

1 Quelle: Wikipedia: http://de.wikipedia.org/wiki/Hacker
2 http://koeln.ccc.de/ablage/artikel/hacker-howto-esr.xml
3 http://www.bsi-fuer-buerger.de/abzocker/05_03.htm
4 http://koeln.ccc.de/ablage/artikel/hacker-howto-esr.xml
5 http://www.bsi-fuer-buerger.de/abzocker/05_03.htm

## 1.2 Bekannte Hacker

### Richard Stallman

Richard Stallman ist bekannt als der Vater freier Software. Als Stallman 1971 anfing, im Labor für künstliche Intelligenz bei MIT zu arbeiten, war er mit 'Geheimnisschutzvereinbarungen' und geschlossenen Programm-quellen konfrontiert, während er hackte und Systemtreiber 'auf traditionelle Weise' verbesserte. Nach einem interessanten Kampf um den Quellcode eines fehlerhaften Druckerprogramms gab Stallman seinen Job auf und wurde der lauteste Fürsprecher für freie Computersoftware und schuf dabei GNU und die Free Software Foundation.[6]

### Linux Torwalds

Linus Torvalds ist bekannt als der Vater von Linux, dem beliebtesten auf Unix basierenden Betriebssystem, das heute in Gebrauch ist. Linus begann mit seiner Arbeit an einem neuen Betriebssystem 1991 und übernahm einige umstrittene Technologien für sein Projekt, nämlich das Konzept der freien Software und das System der öffentlichen Lizenz von GNU.[7]

### Kevin David Mitnick

Kevin Mitnick ist ein US-amerikanischer, weltweit sehr bekannter, ehemaliger Hacker und heutiger Geschäftsführer einer Sicherheitsfirma.

Als Sicherheits-Experte ist Kevin Mitnick alias „Condor“ und ehemaliges Mitglied der „Roscoe Gang“ am meisten durch Social Engineering bekannt geworden. In seiner Karriere soll er unter anderem mehr als 100-mal in das Netzwerk des Pentagon sowie einige Male in das der NSA eingedrungen sein.[8]

### John T. Draper alias Captain Crunch

John T. Draper alias Captain Crunch war einer der populärsten Hacker der 1960er und 1970er Jahre, einer der ersten Phreaker und zudem Mitglied des Homebrew Computer Clubs.

Den Spitznamen Captain Crunch gab sich Draper nach einer in den USA bekannten Frühstücksflocken-Marke namens Cap'n Crunch. Den Packungen lag während einer Werbeaktion eine Spielzeug-Pfeife bei, die einen Ton mit einer Frequenz von 2600 Hertz erzeugen konnte. Wenn man diesen Ton in den Telefonhörer pfiff, war man in der Lage, kostenlose Telefonate zu führen, da zu dieser Zeit Signalisierungsdaten und Sprache auf der gleichen Leitung verliefen (Inband-Signalisierung).[9]

6 http://www.viruslist.com/de/hackers/info?chapter=153350068
7 http://www.viruslist.com/de/hackers/info?chapter=153350068
8 http://de.wikipedia.org/wiki/Kevin_Mitnick
9 http://de.wikipedia.org/wiki/John_T._Draper

### Wau Holland

Wau Holland war ein deutscher Journalist und Computeraktivist. Er gehörte 1981 zu den Gründern des Chaos Computer Clubs (CCC), einem der ältesten Hackerclubs. Ab 1983 arbeitete er als Kolumnist bei der Berliner Tageszeitung, wo er regelmässig über den entstehenden deutschen Computeruntergrund und die Mailboxszene berichtete.[10]

### Karl Koch

Karl Werner Lothar Koch (* 22. Juli 1965 in Hannover; † vermutlich 23. Mai 1989) war ein deutscher Hacker. Koch trat in den Datennetzen unter dem Pseudonym „Hagbard Celine“ (Name einer Hauptfigur der Illuminatus-Trilogie, die Koch stark beeinflusste) auf. Auch seinen Computer hatte er nach dem der Illuminatus-Trilogie („FUCKUP“, „First Universal Cybernetic-Kinetic Ultra-Micro Programmer“) benannt.

Bekannt wurde Koch vor allem durch den so genannten KGB-Hack in den 1980er-Jahren. Dabei arbeitete er mit anderen deutschen Hackern zusammen, die gehackte Informationen von westlichen Computersystemen an das KGB verkauften.

1984 gründete Koch in Hannover einen Ableger des Chaos Computer Club.[11]

## 1.3 Viren, Trojaner, Würmer, Hoax[12]

System Daten auszuspionieren oder gar zu vernichten, kommt jeder PC-Nutzer früher oder später in Kontakt. Solche Schadsoftware bezeichnet man als Malware. Der Begriff setzt sich zusammen aus malicous = schädlich und Software. Zu Malware zählt man unter anderem Viren und Trojanische Pferde. Doch worin unterscheiden sich diese Arten?

### Virus

Viren befallen ausführbare Programm-Dateien, die zum Beispiel mit den Dateinamenserweiterungen ".exe", ".com" oder ".scr" gekennzeichnet sind. Betroffen sind davon fast alle Bestandteile von Windows und installierte Programme. Da diese Viren-Spezies ihren Code in die jeweilige Datei hineinschreiben, wird der Schädling beim Start eines infizierten Programms automatisch mit ausgeführt.

### Makroviren

Makroviren verstecken sich nicht in Programmen, sondern in Word- oder Excel-Dokumenten. Makros werden in einer Office-eigenen Programmiersprache geschrieben; vor allem, um Arbeitsabläufe zu automatisieren. Beim Laden des verseuchten Dokuments beginnt das Virus automatisch mit seiner Schadensroutine. Diese reicht von einfachen Scherzen, wie etwa das Verstecken von Menü-Einträgen, bis hin zum Löschen von Dateien. Hinzu kommt, dass einige Varianten erst an einem bestimmten Tag oder nach einer bestimmten Anzahl von Starts aktiv werden.

### Trojaner

Trojaner, besser Trojanisches Pferd, bezeichnet ein scheinbar harmloses Programm mit einer verdeckten

10 http://de.wikipedia.org/wiki/Wau_Holland
11 http://de.wikipedia.org/wiki/Karl_Koch_(Hacker)
12 http://computer.t-online.de/c/13/46/18/10/13461810.html

Schadensfunktion: einem Virus, Wurm oder Spyware. Der Zweck der meisten Trojaner ist es, schädliche Programme auf den PC zu schleusen, die unbemerkt sensible Daten wie Passwörter für Homebanking oder Mail-Accounts, Kreditkartennummern und ähnliches ausspähen und übermitteln.

## Backdoor-Trojaner

Eine besonders gefährliche Form des Trojanischen Pferdes sind so genannte Backdoor-Trojaner. Hierbei handelt es sich um Hilfsprogramme, durch die ein Hacker auf fremde Rechner zugreifen kann.

## Würmer

Würmer verbreiten sich selbstständig innerhalb eines Netzwerks, sausen jedoch bevorzugt als eMail kreuz und quer durch das Internet, wo sie optimale Bedingungen vorfinden. Im günstigsten Fall besteht ihr Ziel in ihrer endlosen Vermehrung und der Belegung von Speicherressourcen - dadurch sinkt die Rechenleistung eines infizierten PCs. Auch gibt es viele Würmer, deren Code mit den Eigenschaften von PC-Viren kombiniert wurde. Einige haben sogar Trojaner als Schadfracht mit an Bord.

## Spyware

Spyware bezeichnet Programme, die Informationen über PC-Nutzer wie etwa persönliche Daten und Surfgewohnheiten ausspionieren und sie über das Internet übertragen. Die Hintermänner können so zum Beispiel Vorlieben des Surfers erfahren und gezielt Werbung auf den PC schleusen. Spyware-Anbieter locken oft mit hübschen Bildschirmschonern oder anderen attraktiven Gratis-Programmen, in denen sie ihre Schadsoftware verstecken. Zunehmend wird Spyware auch über Trojaner und Würmer verbreitet.

## Hoax

Hoax bedeutet an sich "schlechter Scherz" und wird im Internet für falsche Warnungen vor bösartigen Viren verwendet. Ergänzt wird die Meldung meistens um die Bitte, die eMail an Freunde und Bekannte weiterzuleiten. Hoaxes sind im engeren Sinn keine Malware, denn in der Regel verfolgen sie keine kriminellen Absichten. Dennoch können solche "Scheinviren" gefährlich werden. Einige dieser Hoaxes fordern den PC-Nutzer zum Beispiel auf, bestimmte und zum Teil wichtige System-Dateien zu löschen. Einige Hoaxes geistern schon seit vielen Jahren durchs Internet. Einer der bekanntesten ist der Budweiser Hoax, der vor einem angeblichen Virus in einem Bildschirmschoner der Brauerei warnt.

## Adware

Als Adware bezeichnet man Freeware, die über die Einblendung von Werbung finanziert wird. Die Programme machen in der Regel keinen Hehl daraus, was ihre Absicht ist und bitten den Anwender vor der Installation um Erlaubnis. Da es aber Anwendungen gibt, die zugleich Adware und Spyware sind, stehen alle Vertreter der Klasse Adware unter dem generellen Verdacht, Spyware zu sein.

# 1.4 Antivirus

## 1.4.1 Gehirn einschalten

Anwender sollten niemals unbekannte Dateien oder Programme aus unsicherer Quelle ausführen und generell beim Öffnen von Dateien Vorsicht walten lassen. Das gilt insbesondere für Dateien, die per E-Mail empfangen wurden. Solche Dateien – auch harmlose erscheinende Dokumente wie Bilder oder PDF-Dokumente – können durch Sicherheitslücken in den damit verknüpften Anwendungen auf verschiedene Weise Schadprogramme aktivieren. Daher ist deren Überprüfung mit einem aktuellen Antivirenprogramm zu empfehlen.[13]

## 1.4.2 Betriebssystem-Update

Damit Sicherheitslücken auf einem System geschlossen werden, muss man das System stets auf dem aktuellsten Stand halten. Das Betriebssystem verfügt über eine Updatefunktion, die dies automatisch oder auch auf Wunsch erledigt.

## 1.4.3 Virenschutzprogramme

Antivirenprogramme schützen im Wesentlichen nur vor bekannten Viren. Daher ist es bei der Benutzung eines solchen Programms wichtig, regelmässig die von den Herstellern bereitgestellten aktualisierten Virensignaturen einzuspielen. Viren der nächsten Generation (Tarnkappenviren) können von Antivirensoftware fast nicht mehr erkannt werden. Mit Hilfe dieser Programme werden Festplatte und Arbeitsspeicher nach schädlichen Programmen durchsucht. Antivirenprogramme bieten meist zwei Betriebsmodi: einen manuellen, bei dem das Antivirenprogramm erst auf Aufforderung des Benutzers alle Dateien einmalig überprüft (on demand) und einen automatischen, bei dem alle Schreib- und Lesezugriffe auf die Festplatte und teilweise auch auf den Arbeitsspeicher überprüft werden (on access).

Werden mehrere On-Demand-Scanner installiert und – auch unabhängig, also nicht gleichzeitig – gestartet und ausgeführt, sind falsche Virenfunde häufig, bei denen das eine Programm die Virensignaturen des anderen auf der Festplatte oder im Arbeitsspeicher als Virus erkennt bzw. schon gesicherte Virendateien im so genannten „Quarantäne-Ordner“ des anderen Programms findet.[14]

## 1.4.4 Antiviren-Update

Es ist wichtig, sich regelmässig Updates des Antivirus-Programms zu besorgen, wenn man bedenkt, wie schnell sich Bedrohungen heutzutage ausbreiten. Den Vertreibern von Antivirus-Programmen ist es gelungen, die Zeit zwischen den einzelnen Virus-Updates deutlich zu verkürzen: wo es zuerst vierteljährliche, dann monatliche und später wöchentliche Updates gab, sind sie nun zu täglichen Updates übergegangen.

Bessere Funktionalität des Antivirus-Programms kann auch Teil eines solchen Updates sein.

## 1.4.5 Funktionsweise von einem Antivirenprogramm

### Signaturenanalyse

Fast alle Antivirus-Programme arbeiten mit der Signaturenanalyse, d.h. sie nutzen eine Datenbank, die Bytesequenzen von bekannten Viren, Würmern, Trojanern oder anderen Malicious Codes enthält. Sobald es

13 http://de.wikipedia.org/wiki/Computervirus
14 http://de.wikipedia.org/wiki/Computervirus

neue Virussignaturen gibt, werden die Antivirus-Datenbänke entsprechend ergänzt. Die Virenfachleute erweitern die Datenbank um rund 200 neue Virusinformationen pro Tag. Diese Informationen werden den Nutzern als Updates zugänglich gemacht, damit sie ihre Computer noch besser schützen können.

Die Signaturenanalyse ist jedoch nicht die einzige Schutzmassnahme, die zur Verfügung steht. Über die Jahre sind Antivirus-Lösungen immer weiter entwickelt worden, um der zunehmenden Komplexität der Störangriffe zu begegnen. Proaktive Erkennungsmechanismen wurden entwickelt, die Bedrohungen auffinden sollen, bevor sie sich auf dem Rechner bemerkbar machen. Auch Heuristik, Generic Detection und Behavior-Analysen gehören zu den ersten Schutzmassnahmen.

### Heuristik

Das Wort Heuristik leitet sich aus dem griechischen Wort für ‚ich finde' ab. Man bezeichnet damit eine Lernmethode, die auf Spekulationen und Vermutungen basiert und weniger auf festen Algorithmen. Im Bereich der Antivirus-Software setzt die Heuristik nicht-spezifische Entdeckungsmethoden ein, um neue, bisher nicht bekannte Malware zu finden.

Mit dieser Technik, die schon seit vielen Jahren in Gebrauch ist, untersucht man den Code einer Datei (oder eines anderen Objekts), um festzustellen, ob darin virusähnliche Befehle enthalten sind. Sobald die Anzahl von virusähnlichen Befehlen ein vorher festgelegtes Mass überschreitet, wird die entsprechende Datei als möglicherweise virusinfiziert markiert und der Kunde wird aufgefordert zur weiteren Analyse ein Muster einzuschicken. Die Heuristik ist über die Jahre immer weiter verbessert worden und hat schon viel dazu beigetragen, neue Bedrohungen zu entdecken.

### Generic Detection

Generic Detection bezeichnet die Erkennung und Entfernung von Mischviren mit Hilfe einer einzelnen Virussignatur. Ausgangspunkt für die Generic Detection ist die Tatsache, dass erfolgreiche Viren oft von ihrem eigenen Ersteller noch weiter verfeinert oder von anderen Virenschreibern kopiert werden. Daraus resultiert eine Flut von Viren, Würmern und Trojanern, die sich zwar voneinander unterscheiden, aber doch derselben Familie angehören. In manchen Fällen kann die Zahl der Variationen zwei- oder gar dreistellige Grössenordnungen annehmen.

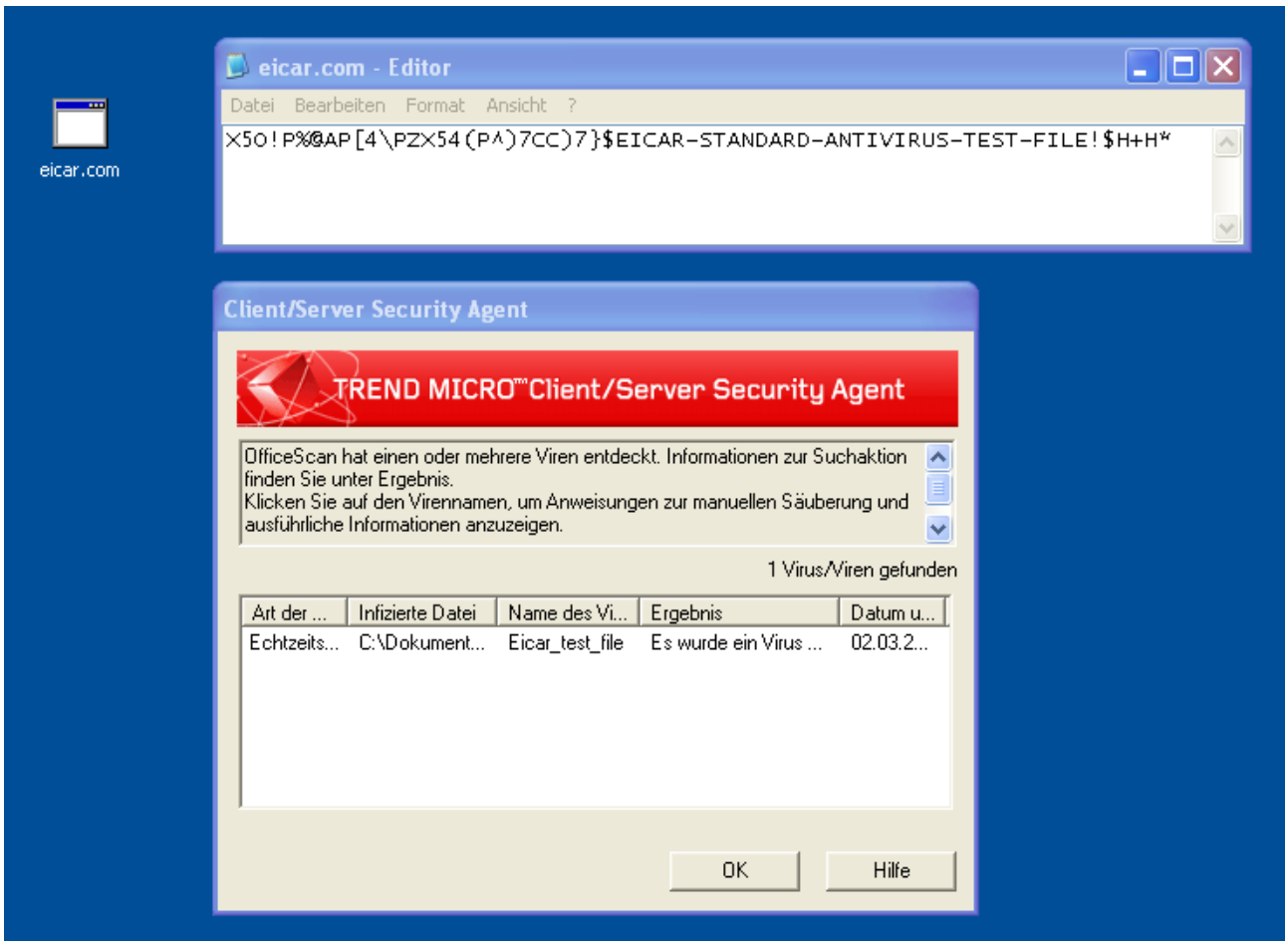
## 1.4.6 EICAR-Testsignatur

EICAR e.V. ist ein gemeinnütziger Verein mit dem Ziel, Computerviren zu erforschen und die Entwicklung von Antivirensoftware zu verbessern. Ursprünglich stand das Akronym EICAR für European Institute for Computer Antivirus Research, ist jedoch heute ein Eigenname. Die Organisation hat ihr Arbeitsgebiet erweitert und befasst sich heute mit nahezu allen Gebieten der Informationssicherheit. EICAR bezeichnet sich deshalb seit einiger Zeit auch als European Expert Group for IT-Security.

Der 1990 gegründete Verein hat seinen Sitz in München. Er verfolgt seine Ziele durch Kongresse, Expertenforen, Task Forces und Beratungsgremien (Advisory Boards).

Bekannt ist das EICAR vor allem für die dort entwickelte EICAR-Testdatei, die zum Testen der Funktion von Antiviren- und Anti-Malware-Software eingesetzt wird.[15]

15 EICAR.2009. http://de.wikipedia.org/wiki/EICAR (Besucht am 3.02.2009)




In der ausführbaren Datei eicar.com steckt der Text, der im Editor zu sehen ist. Dieses Muster ist in der Signaturdatenbank des Antivirenprogramms als Schädling eingetragen. Deshalb

# 1.5 Firewall[16]

## 1.5.1 Hardware oder Software?

### Personal Firewall

Sie kontrolliert die Verbindung zwischen dem PC und dem Netzwerk, an dem der PC angeschlossen ist und ist somit in der Lage, Netzwerkzugriffe zwischen dem PC und dem Internet genauso zu filtern, wie die Zugriffe zwischen dem PC und dem lokalen Netz. Die Installation auf dem zu schützenden Rechner erlaubt es auch, anwendungsspezifisch oder nach Benutzerkennungen zu filtern. Der direkte Zugriff auf das zu überwachende System erweitert die Möglichkeiten dieser Software ungemein. Im Umkehrschluss haben allerdings auch Programme, welche auf derselben Hardware wie die Firewall laufen, wesentlich mehr Möglichkeiten diese zu manipulieren und zu umgehen, als bei einer externen Firewall. Daher kann die Desktop-Firewall eine externe Firewall lediglich ergänzen, jedoch nicht ersetzen.

Die Schutzwirkung von Personal Firewalls ist umstritten, da sie einerseits unerwünschten Datenverkehr erschweren, andererseits auch durch Fehler im eigenen Code den Rechner unsicher machen könnten.

16 http://de.wikipedia.org/wiki/Firewall

### Hardware Firewall

Eine externe (Netzwerk- oder Hardware-) Firewall stellt eine kontrollierte Verbindung zwischen zwei logischen Netzen her. Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall das private Netzwerk bzw. das Netzsegment vor unerlaubten Zugriffen zu schützen.

Von Regelverstössen einmal abgesehen, besteht die Funktion einer Firewall nicht darin, Angriffe zu erkennen und zu verhindern. Sie besteht lediglich darin, nur bestimmte Kommunikationsbeziehungen – basierend auf Absender- oder Zieladresse und genutzten Diensten – zu erlauben.

### Intrusion Detection System

Für das Aufspüren von Angriffen sind so genannte IDS-Module zuständig, welche durchaus auf einer Firewall aufsetzen können. Sie gehören jedoch nicht zum Firewallmodul.

## 1.5.2 Sinn und Zweck

## 1.5.3 Vor was schützen Firewalls nicht?

Personal Firewalls zeigen gegen Viren keine Wirkung, da ihre Funktionalität auf die Arbeitsweise von Würmern zugeschnitten ist und Viren nicht beeinträchtigt.

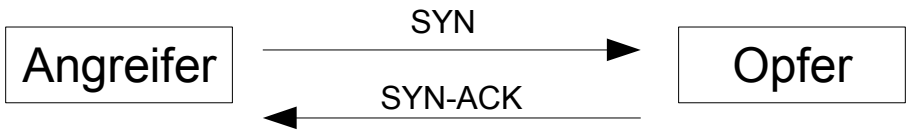
Da sie nur den Netzwerkverkehr an wenigen Stellen filtern, bieten sie keinen Schutz vor Schädlingen, die über Laptops, USB-Sticks oder Disketten in das interne Netz gebracht werden.

## 1.5.4 Woher kommen die Angriffe

## 1.5.5 Angriffsarten

### Die SYN-Flood Attacke

Die SYN-Flood Attacke ist eine Denial of Service Attacke. Dabei wird der Verbindungsaufbau des TCP-Transportprotokolls verwendet. Bei erfolgreicher Attacke sind Dienste oder ganze Computer in einem Netzwerk nicht mehr erreichbar. DOS-Attacken haben das Ziel, das Zielsystem zu überlasten.




Bei der SYN-Flood-Attacke wird die ACK-Nachricht nicht gesendet. Das Opfer wartet auf die Antwort vom Angreifer. Die Verbindung ist noch halb offen, also noch nicht ganz abgeschlossen. Der Speicherbereich im Netzwerkstack bleibt aber weiterhin reserviert. Wenn man sehr viele Verbindungsanfragen stellt, ohne diese zu bestätigen überläuft schlussendlich der Speicher vom Opfer.

Als Gegenmassnahme können SYN-Cookies oder Firewalls dienen.

## 1.5.6 Firewall-Typen

### Bridging-Firewall

Hier sind die Netzwerkschnittstellen wie bei einer Bridge gekoppelt. Derartige Geräte sind, genau wie Bridges oder Switches, im Netz nicht sichtbar, also für einen Angreifer nur schwer zu erkennen und darüber hinaus nur schwer anzugreifen. Denn dieser Typ Firewall hat keine offenen Ports und ist lediglich indirekt über Fehler im Bridging-Code angreifbar. Auf der anderen Seite kann sie lediglich als statischer Paketfilter eingesetzt werden und ist nicht in der Lage, eine Adressumsetzung vorzunehmen, wie das beispielsweise bei einer Verbindung zwischen dem privaten Netz und dem Internet vonnöten ist.

### Routing-Firewall

Hier sind die Netzwerkschnittstellen wie bei einem Router gekoppelt. Das ist die am weitesten verbreitete Art; sie kommt bei praktisch allen SoHo-Geräten (für den privaten Gebrauch und kleinere Unternehmen), aber mitunter auch bei größeren Systemen zum Einsatz. Ein Nachteil ist, dass diese Firewall im Netz sichtbar ist und direkt angegriffen werden kann. Entweder erscheint sie als Verbindungsglied zwischen den Subnetzen (Router ohne NAT), oder aber sie wird gar als vermeintlicher Kommunikationspartner angesprochen (Router im NAT-Modus). Im NAT-Modus bildet diese Firewall ihre eigene externe Adresse auf den jeweiligen internen Client ab, der eine Verbindung zum externen Netz (Internet) hergestellt hat. Bildlich gesehen funktioniert sie dann wie ein automatisiertes Postfach, welches alle ausgehenden Pakete, die die Firewall passieren, mit der eigenen Absenderadresse versieht. Dadurch stellt sie sicher, dass das Zielsystem die Antwortpakete auch wieder an das „Postfach“ schicken wird. Dank einer speziellen NAT-Verwaltung (PAT) erkennt sie, zu welchem internen Gerät ein aus dem Internet eingehendes Antwortpaket gehört. Dorthin leitet sie das Paket weiter, ohne dass der Versender aus dem Internet die wirkliche (interne) Adresse seines Kommunikationspartners kennt. In diesem Modus verdeckt sie – genau wie eine Proxy-Firewall – die Struktur des internen Netzes, ist im Unterschied dazu aber nicht in der Lage, die Verbindung zu beeinflussen.

### Proxy-Firewall

Hier arbeitet die Firewall als Proxy zwischen dem Quell- und Zielsystem und tritt grundsätzlich für wenigstens einer der beiden Seiten selbst als vermeintlicher Kommunikationspartner in Erscheinung. Im Unterschied zur Routing-Firewall terminiert sie die Verbindungen auf beiden Seiten (es handelt sich somit um zwei eigenständige Verbindungen), was bedeutet, dass sie die Kommunikation nicht einfach weiterleitet, sondern selbst führt. Daher kann sie den Inhalt der Netzwerkpakete zusammenhängend analysieren, Anfragen filtern und bei Bedarf beliebige Anpassungen vornehmen, aber auch entscheiden, ob und in welcher Form die Antwort des Ziels an den tatsächlichen Client weitergereicht wird.

## 1.5.7 Firewallösung

### Variante 1

### Variante 2

### Variante 3

**Variante 4**

# 1.6 DMZ

Eine Demilitarized Zone bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (Bastion Hosts mit z. B. E-Mail, WWW o. ä.) gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen.

### Exposed Host als „Pseudo-DMZ“

Einige Router für den Heimgebrauch bezeichnen die Konfiguration eines Exposed-Host fälschlicherweise als „DMZ“. Dabei kann man die IP-Adresse eines Rechners im internen Netz angeben, an den alle Pakete aus dem Internet weitergeleitet werden, die nicht über die NAT-Tabelle einem anderen Empfänger zugeordnet werden können. Dieses Verfahren stellt ein erhebliches Sicherheitsrisiko dar. Es eignet sich eher für die Fehlersuche, um temporär den Einfluss der Firewall zu umgehen, etwa bei Problemen mit bestimmten Datenverbindungen. Ein Port-Forwarding der tatsächlich benutzten Ports ist dem vorzuziehen.

Es hängt von der konkreten Konfiguration der Firewall ab, ob zunächst Port-Forwardings auf andere Rechner berücksichtigt werden und erst danach der Exposed Host, oder ob der Exposed Host die Port-Forwardings auf andere Rechner unwirksam macht.

### Was kommt in eine DMZ?

Dienste, die von aussen her erreichbar sein sollen, werden in die DMZ gestellt. Folgendes wäre zum Beispiel möglich:

- Webserver
- FTP-Server
- Mailserver
- Webmail-Oberfläche

## 1.6.1 Extranet

Das Extranet nach ISO/IEC 2382 ist eine Erweiterung des Intranets um eine Komponente, die nur von einer festgelegten Gruppe externer Benutzer verwendet werden kann. Extranets dienen der Bereitstellung von Informationen, die zum Beispiel Unternehmen, Kunden oder Partnern zugänglich gemacht werden, nicht aber der Öffentlichkeit.[17]

Das Extranet kann man also als ein Intranet bezeichnen, das auch von ausserhalb zugänglich ist. Damit nicht alle Leute auf dieser Welt darauf Zugriff haben, muss man sich oft authentifizieren.

17 http://de.wikipedia.org/wiki/Extranet

### 1.6.2 Intranet

Ein Intranet ist ein organisations- oder unternehmensinternes, nicht-öffentliches Rechnernetzwerk, das auf den gleichen Techniken (TCP/IP, HTTP) und Anwendungen wie das Internet basiert und den Mitarbeitern einer Unternehmung oder Organisation als Informations-, Kommunikations- und Anwendungsplattform zur Verfügung steht. Innerhalb eines Intranets können auch Verzeichnisdienste zur Verfügung gestellt werden.[18]

## 1.7 Breitbandtechnologien

### 1.7.1 Was ist Breitband?

Ein Breitband-Internetzugang (auch Breitbandzugang, Breitbandanschluss) ist ein Zugang zum Internet mit verhältnismäßig hoher Datenübertragungsrate von einem Vielfachen der Geschwindigkeit älterer Zugangstechniken wie der Telefonmodem- oder ISDN-Einwahl, die im Unterschied als Schmalbandtechniken bezeichnet werden.

In vielen Gebieten findet in den frühen 2000er Jahren ein starkes Wachstum des Marktes für Breitbandzugänge statt.

Es existiert keine eindeutige Definition, ab wann eine breitbandige Verbindung beginnt – der Begriff wird (besonders im Marketing der Telekommunikationsindustrie) verwendet.

Ursprünglich wurde mit Breitband eine Realisierungsform von Datennetzwerken bezeichnet, die heute aber veraltet ist.

### 1.7.2 Was sind Breitbandtechnologien?

#### Telefonnetz

Eine der verbreitetsten Technologien arbeitet mit einer verbesserten Nutzung der Kupferleitungen des Telefonnetzes, da durch die bestehende Infrastruktur geringere Neuinvestitionen nötig sind. Dabei sind in erster Linie die hauptsächlich verwendeten DSL-Techniken zu nennen. Es gibt oder gab jedoch auch andere Ansätze, wie die Entwicklung schnellerer Telefonmodems oder eines schnelleren ISDN-Standards, dem Breitband-ISDN (B-ISDN).

DSL-Technologien sind nur zur Überbrückung kurzer Distanzen geeignet, was – je nach Übertragungsgeschwindigkeit – nach wenigen hundert Metern oder erst wenigen Kilometern den Übergang zu einer anderen Übertragungstechnik oder DSL-Verstärker oder Repeater nötig macht. Daher handelt es sich in der Regel um eine Hybridtechnik in Kombination mit, wie in den meisten Fällen, Glasfasern oder beispielsweise auch Richtfunkstrecken. Mit wachsenden Übertragungsraten rückt der Übergabepunkt immer näher an den Endnutzer.

Eine andere Möglichkeit für breitbandige Datenübertragungen über Telefonleitungen ist die Bündelung mehrerer analoger oder ISDN-Leitungen, was hauptsächlich in Ermangelung des in vieler Hinsicht überlegenen DSL genutzt wurde oder teils noch wird.

#### Kabelfernsehnetz

Die Daten werden mit Kabelmodems auf die analogen Signale des Kabelfernsehnetzes aufmoduliert und so über diese Koaxialkabel übertragen. Auch hier handelt es sich aus ähnlichen Gründen wie bei DSL in der Regel um eine Hybridtechnik. Momentan werden Geschwindigkeiten bis zu 32 MBit/s im Downstream und 2,5 MBit/s im Upstream angeboten.[6]

18 http://de.wikipedia.org/wiki/Intranet

## Direkte Glasfaseranbindung

Den Endkunden direkt per Glasfaser anzubinden ermöglicht hohe Bandbreiten über große Entfernungen. Notwendige Verlegungen neuer Anschlüsse zu jedem Kunden machen dies jedoch sehr kostspielig. Siehe auch Fibre To The Basement, Fiber To The Home

## Elektrizitätsnetz / PowerLine

Mittels Trägerfrequenzanlagen (TFA) können Internetzugänge über das Stromnetz realisiert werden, auch unter dem englischsprachigen Begriff Powerline Communication (PLC) bekannt. Meist werden damit Datenverbindungen zwischen heimischen Steckdosen und z. B. Trafostationen realisiert, die über Glasfaser oder Richtfunk angebunden werden.

## Terrestrische Funktechnologien

Sind eine Möglichkeit, breitbandigen Datenaustausch zu ermöglichen.

Vielerorts – insbesondere wo keine Versorgung mittels herkömmlichen Kabeltechnologien gegeben ist – bauen sogenannte Wireless Internet Access Provider sogenannte Wireless Metropolitan Area Networks (WMAN) auf, um darüber einen schnellen Internetzugang anbieten zu können. Dabei kommen unterschiedliche Technologien zum Einsatz, darunter der speziell entwickelte WiMAX-Standard, Wireless Local Area Network (WLAN)-Technologien, sowie verschiedene proprietäre Lösungen, die teils unter Namen wie Funk-DSL oder Wireless DSL vertrieben werden.

Mehr oder weniger breitbandige Datendienste können auch Mobilfunkstandards wie HSDPA, UMTS oder EDGE bieten.

Unter Umständen kann auch Packet Radio aus dem Amateurfunkbereich dazugezählt werden. Hiermit können Übertragungsraten von bis zu mehreren Megabit pro Sekunde realisiert werden und entsprechende Übergabepunkte können auch Zugang zum Internet ermöglichen. Die Nutzung ist jedoch Funkamateuren vorbehalten.

## Internetzugang über Satellit

Reine Satellitenverbindungen (2-Wege-Satellitenverbindung) sind unabhängig von landschaftlichen Gegebenheiten oder anderer Infrastruktur praktisch überall auf der Erdoberfläche verfügbar und eignen sich damit besonders für entlegene Gebiete und Schiffe.

Problematisch sind bei Satellitenzugängen die immer noch oft deutlich höheren Kosten, die hohen Latenzzeiten und, sofern der Rückkanal nicht über den Satellit realisiert ist, die Abhängigkeit von einer weiteren Zugangsmöglichkeit. Im Beispiel eines Systems mit geostationären Satelliten ergeben sich typische Verzögerungen von 500–700 ms, was Echtzeitanwendungen empfindlich stört.

## Hochfliegende Luftfahrzeuge

Über hochfliegende stationäre Luftschiffe können Funksignale für Dienste wie Fernsehausstrahlung, Mobiltelefonie oder eben auch Internetzugänge vermittelt werden. Ein Beispiel für eine Umsetzung dieser Technologie trägt den Markennamen Stratellite.

Ein weiterer Ansatz wären hochfliegende unbemannte (Leicht)Flugzeuge wie Helios.

## 1.7.3 DSL-Unterschiede[19]

Es gibt verschiedene Arten von DSL-Techniken, die unter der Bezeichnung „DSL“ oder „xDSL“ (x als Platzhalter für das spezifische Verfahren) zusammengefasst werden:

### ADSL

Asymmetric Digital Subscriber Line, eine asymmetrische Datenübertragungstechnologie, zum Beispiel mit Datenübertragungsraten von 8 Mbit/s zum Teilnehmer (Downstream) und 1 Mbit/s in der Gegenrichtung (Upstream);

### ADSL2+

Eine erweiterte Form von ADSL mit Datenübertragungsraten von bis zu 25 Mbit/s zum Teilnehmer (Downstream) und bis zu 3,5 Mbit/s in der Gegenrichtung (Upstream), die Geschwindigkeit wird dynamisch ausgehandelt;

### HDSL

High Data Rate Digital Subscriber Line, eine symmetrische Datenübertragungstechnik mit Datenübertragungsraten zwischen 1,54 und 2,04 Mbit/s;

### SDSL (G.SHDSL)

Symmetrical Digital Subscriber Line, eine symmetrische Datenübertragungstechnologie mit Datenübertragungsraten von bis zu 3 Mbit/s symmetrisch, das heißt sowohl in Empfangs- wie in Senderichtung; bei vieradriger Anschaltung (zwei Kupfer-Doppeladern) können maximal 4 Mbit/s übertragen werden. Alternativ kann auch die Reichweite auf Kosten der Datenrate erhöht werden.

### VDSL bzw. VDSL2

Very High Data Rate Digital Subscriber Line, eine Datenübertragungstechnologie, die theoretisch Datenübertragungsraten von bis zu 210 Mbit/s im symmetrischen Betrieb bietet.

### Andere als „DSL“ bezeichnete Verfahren

- ISDN Digital Subscriber Line verwendet vorhandene ISDN-Technik und ermöglicht Datenraten bis zu 160 kbit/s
- cableDSL – Markenname der TELES AG für einen speziellen Internetzugang über Kabelanschluss
- skyDSL – Markenname der TELES AG für einen europaweit flächendeckend verfügbaren Internetzugang über Satellit mit bis zu 24 Mbit/s im Downstream
- T-DSL via Satellit – Markenname der Deutschen Telekom für einen Internetzugang über Satellit. Der Zugang über den Satelliten ermöglicht bei den genannten Produkten lediglich den Empfang von Daten, zum Senden wird ein herkömmliches Modem oder eine ISDN-Verbindung verwendet.
- Wireless Digital Subscriber Line (WDSL) verwendet Funk-Technik und ermöglicht Datenraten bis zu 512 Mbit/s. Es wird unter diesen Namen von der Firma FPS InformationsSysteme GmbH genutzt.
- mvoxDSL – Markenname für ein Internet via Funk – Angebot der Firma mvox AG

19 http://de.wikipedia.org/wiki/Digital_Subscriber_Line

- FlyingDSL – Markenname für ein Internet via Funk – Angebot der Firma Televersa online
- PortableDSL – Markenname für Internet via Funk – Angebot der Firmen isomedia und Airdata
- AvioDSL – Markenname für Internet via Funk – Angebot der Firma overturn technologies gmbh
- smart-DSL – Markenname für Internet via Funk – Angebot der Firma smartup solutions GmbH

# 1.8 Verbindungsarten

## 1.8.1 Standleitung / Festverbindung[20]

Eine Standleitung ist eine permanente (dauerhaft stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz. Im Gegensatz zu einer Wählleitung steht der gesamte Übertragungsweg immer zur Verfügung.

Über die Verbindung können Daten jeder Art übertragen werden, beispielsweise analoge (z. B. Telefongespräch) oder digitale (z. B. Datendirektverbindung). Die Verbindung selbst kann dabei physisch ausgeführt sein, z. B. als Kupfer-Doppelader von Endgerät zu Endgerät, oder virtuell, als Teil einer übergeordneten Infrastruktur wie SDH oder ATM-Virtual Circuit. Der Anschluss einer Datenstandleitung ist bittransparent.

Der Ausdruck Standleitung wird teilweise auch benutzt, um eine lang dauernde Verbindung beliebiger Art und Qualität zu bezeichnen. Die einfachste Form einer solchen (nicht anbieterseitig geschalteten) Standleitung ist eine dauerhaft hergestellte Wählleitung über das Telefonnetz. Hier werden die Modems der Teilnehmer so programmiert, dass sie sich gegenseitig anwählen.

Die Abrechnung geschieht oft per verbrauchtes Datenvolumen.

### Medien / Geschwindigkeit

- Kupferleitung: 2 Mbit/s
- Lichtwellenreiter: 10 Mbit/s bis 100 Mbit/s
- Es sind auch Geschwindigkeiten bis zu 16 Gbit/s erreichbar

### Standleitung ins Internet

Für den Anschluss an das Internet wird – speziell von Firmen – häufig eine Standleitung verwendet. Wird auf diese Weise über eine Standleitung ein Netz mit dem Internet verbunden, so enthält dies in der Regel auch die Zuweisung mindestens einer festen, öffentlichen IP-Adresse. Diese Standleitungen eignen sich dann besonders, um Server im Internet zu betreiben.

### Permanenter DSL-Anschluss

Die Verbindung über ein DSL-Modem ins Internet wird gelegentlich als Standleitung bezeichnet, etwa echte (S)DSL-basierte Standleitungen, wie sie z. B. Arcor oder QSC anbietet. Quasi-permanente Leitungen mit regelmäßiger Zwangstrennung und wechselnder IP-Adresse, wie sie z. B. die Deutsche Telekom anbietet, sind keine Standleitungen.

20 http://de.wikipedia.org/wiki/Standleitung

### 1.8.2 Wählverbindung[21]

Eine Wählleitung ist eine Telekommunikationsleitung, mit der mittels eines Signalisierungsverfahrens eine Verbindung zu einer bestimmten Gegenstelle aufgebaut werden kann. Fortgeschrittene Dienste wie ISDN eröffnen zahlreiche Möglichkeiten bzgl. des Umganges mit Wählleitungen wie das Umlegen eines Anrufes auf andere Endgeräte oder Konferenzschaltungen.

Der schmalbandige Internetzugang, bei dem der Rechner ein Telefonmodem oder ein ISDN-Endgerät benutzt, um den Internetdienstanbieter (ISP) über das Telefonnetz anzuwählen, wird umgangssprachlich auch so genannt. Die Einwahl (engl. dial-in bzw. dial-up) geschieht hier zum Verbindungsaufbau mit einem Einwahlknoten, der unmittelbar mit dem Internet verbunden ist.

### 1.8.3 VPN

| Funktion | Kategorie | Intern / Extern // Info |
|---|---|---|
| Tunnel-Mode | Übertragungsmodus | Extern, da Gesamtes IP-Paket verschlüsselt // LAN-LAN; Host-LAN, Host-Host |
| Transport Mode | Übertragungsmodus | Intern, da nur Nutzlast verschlüsselt // Nur Host-Host |
| AH | Sicherheitsprotokoll | Intern, da nicht verschlüsselt |
| ESP | Sicherheitsprotokoll | Extern, da verschlüsselt |
| Main Mode | Verbindungsaufbau | Extern, da verschlüsselt (dafür langsamer) |
| Aggressive Mode | Verbindungsaufbau | Intern, da nicht verschlüsselt (dafür schneller) |
| PSK | Verschlüsselungsverfahren | Intern, da nur ein Schlüssel // Symmetrisch (Schneller) |
| PKI | Verschlüsselungsverfahren | Extern, da besserer Überblick / Kontrolle // Asymmetrisch |
| PFS | | Extern, da es sicherer ist und nur mit PKI verwendbar ist. |

21 http://de.wikipedia.org/wiki/W%C3%A4hlleitung

### 1.8.4 VPN-Arten im Überblick

| VPN-Art | Vorteile | Nachteile |
|---|---|---|
| IPSec | Zugriff nur von erlaubten Rechnern aus möglich<br>Access Policies und unternehmensweite Sicherheitsrichtlinien (z.B. Virenschutz) wirksam<br>Kompletter Zugriff auf Unternehmensressourcen und Anwendungen | Bindet Benutzer an bestimmte Rechner<br>Erfordert umfangreichere Benutzerverwaltung<br>Firewalls und NAT kann den Zugriff verhindern |
| OpenVPN | Sicher und einfach zu konfigurieren<br>Port, Protokoll, etc. frei wählbar<br>Hohe Kompatibilität mit Firewalls, Proxies, …<br>Nur ein, frei wählbarer Port notwendig<br>HTTPS – Jeder Proxy kann getunnelt werden<br>Umfangreiche Scripting-Möglichkeiten<br>Flexible Netzwerkkonfiguration<br>High Performance<br>Einfache Installation und Konfiguration<br>Verfügbar für alle Plattformen | Da das Projekt OpenSource ist, können von Programmierern absichtlich Sicherheitslücken eingebaut werden. Diesen Vorfall hat es schon einmal gegeben. |
| PPTP | Verfügbarkeit - Da PPTP im Lieferumfang von Windows (ab NT) enthalten ist, ist es ohne Zusatzsoftware unmittelbar verfügbar.<br>Simple Einrichtung.<br>Diverse Protokolle nutzbar (IP, NetBEUI, IPX) | Defizite bei der Schlüsselverwaltung (Sicherheit)<br>Nicht mehr sicher ohne Zertifikate |
| SSL-VPN | Vielfalt an Webbrowser ermöglicht fast universellen Zugriff<br>Erlaubt dedizierten Zugriff auf Applikationsebene<br>Einfacher Zugriff auf webbasierte Anwendungen<br>In der Regel geringere Kosten (TCO) als IPSec<br>Einfachere Skalierbarkeit | Zugriff von nicht gesicherten Rechnern möglich<br>Token oder digitale Zertifikate werden benötigt um Angriffe auf das Passwort zu verhindern.<br>Sensible Informationen können auf unsicheren Rechnern zurückgelassen werden<br>Wenige Applikationen unterstützen out-of-the-box webbasierten Zugriff. |
| Hamachi | Verschlüsseltes Instant Messaging (AES-256)<br>Sicherer Datei Tausch über virtuelles LAN<br>Das Spielen von Games über virtuelles LAN! | Freigaben welche im LAN freigegeben wurden, werden automatisch auch im Hamachi Netzwerk freigegeben<br>Zu unsicher für Geschäftsumfeld<br>Langsamer, da es immer über einen Hamachi-Server geht. |

### 1.8.5 RAS - Remote Access Service[22]

Mit dem Remote Access Service (von engl. remote, „entfernt, fern“, access, „Zugriff“ und service, „Dienst”) bietet Microsoft Windows NT die Möglichkeit, Clients über eine Modem-, ISDN- oder X.25-Verbindung mit dem lokalen Netzwerk zu verbinden. Dabei werden nicht nur unterschiedliche Clients unterstützt, sondern es besteht auch eine große Flexibilität in der Auswahl und Kombinationsmöglichkeit der verwendeten Netzwerkprotokolle.

Die über RAS mit dem NT-Netzwerk verbundenen Clients können auf die gesamte Funktionalität des Netzwerkes zurückgreifen, als wären sie direkt lokal mit dem Netzwerk verbunden.

## 1.9 Paketvermittelnde Dienste

### TCP/IP-Protokoll

### Grundlegende Eigenschaften von TCP

1. End-zu-End Verbindung
2. Verbindngsmanagement
3. Zeitüberwachung
4. Fehlerbehandlung
5. Flusskontrolle
6. Zuverlässig

Unmöglich ist

- Streaming

### Paketvermittelnde Dienste

<tbd: was ist darunter zu verstehen?>

## 1.10 Ports

### 1.10.1 TCP/IP-Stack im OSI-Modell

| TCP/IP-Schicht | ≈ OSI-Schicht | Beispiel |
|---|---|---|
| Anwendungsschicht | 5–7 | HTTP, FTP, SMTP, POP, Telnet |
| Transportschicht | 4 | TCP, UDP |
| Vermittlungsschicht | 3 | IPv4,IPv6 |
| Netzzugangsschicht | 1–2 | Ethernet, Token Bus, Token Ring, FDDI |

22 http://de.wikipedia.org/wiki/Remote_Access_Service

### 1.10.2 Unterschiede TCP und UDP

| Aspekt | TCP | UDP |
|---|---|---|
| Aufbau des Headers | Umfangreich<br>ACK-Nr; SEQ-Nr. | Einfach |
| Handshake-Verfahren | Verbindung wird formell aufgebaut | Verbindung wird nicht formell aufgebaut |
| Verbindungsverfahren | Verbindungsorientiert | Verbindungslos |
| Anwendungsprotokolle | SMTP, POP3, Telnet, FTP, ... | DNS, RDP, DHCP |
| Typisch für die Anwendungsprotokolle | | Ziel muss im Moment des Verbindungsaufbaus nicht erreichbar sein. |
| Besondere Kommunikationsart | - | Kommunikationsart, die nur von UDP betrieben werden kann: Streaming |

### 1.10.3 Portliste

| Nr. | Dienst | Beschreibung |
|---|---|---|
| 7 | Echo | Zurücksenden empfangener Daten |
| 20 | FTP-Data | Dateitransfer (Datentransfer vom Server zum Client) |
| 21 | FTP | Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client) |
| 22 | SSH | Secure Shell |
| 23 | Telnet | Terminalemulation |
| 25 | SMTP, ESMTP | E-Mail-Versand (siehe auch Port 465) |
| 42 | Nameserver | Host Name Server (TCP und UDP) |
| 43 | Whois | Whois-Anfragen |
| 53 | DNS | Auflösung von Domainnamen in IP-Adressen |
| 67 | BOOTPS | BootStrap Protokoll server, auch genutzt von DHCP-Anfrage |
| 68 | BOOTPC | BootStrap Protokoll client, auch genutzt von DHCP-Antwort |
| 80 | HTTP | Webserver |
| 110 | POP3 | Client-Zugriff für E-Mail-Server |
| 119 | NNTP | Usenet (Newsgroups) |
| 123 | NTP | Zeitsynchronisation zwischen Computern |
| 143 | IMAP | Zugriff und Verwaltung von Mailboxen |
| 161 | SNMP (UDP) | Überwachung und Steuerung von Netzwerkelementen |
| 443 | HTTPS | Verschlüsselte Webserver Übertragung, meist mit SSL- oder TLS-Verschlüsselung |
| 445 | Microsoft-DS | Microsoft Directory Server, Windows Dateifreigabe |
| 465 | SMTPS | gesicherter E-Mail-Versand |
| 993 | IMAPS | gesicherter Zugriff und Verwaltung von Mailboxen |

| | | |
|---|---|---|
| 995 | POP3S | gesicherter Client-Zugriff für E-Mail-Server |
| 1723 | PPTP | Point-to-Point Tunneling Protocol VPN |
| 3306 | MySQL | Zugriff auf MySQL-Datenbanken |
| 3389 | RDP | Windows Remotedesktopzugriff, Windows Terminal Services |
| 5060 | SIP | IP-Telefonie |
| 5800 | VNC | Virtual Network Computing (Port für Java-Zugriff) |
| 5900 | VNC | Virtual Network Computing (Port für VNC Viewer-Zugriff) |
| 6667 | IRC | Chatserver |
| 10000 | Webmin | Webmin - Web-basierende Oberfläche für Systemadministratoren unter Linux |
| 20000 | Usermin | Oberfläche für Systemadministratoren unter Linux (ähnlich Webmin) |

# 1.11 Subnetze / IP-Rechnen mit der ultimativen Master-Table

## 1.11.1 Schritt 1: Generate your own mastertable

1. Alternative Schreibweise der Subnetzmaske: Von 0 bis 8 durchnummerieren.
2. Die dezimale Schreibweise darunter schreiben. Wenn 1 Bit bei der Subnetzmaske gesetzt ist, dann ist ein Subnetz 128 gross. Bei 2 ist es um die Hälfte grösser.
   Also: 1 → 128 und dann immer + die Hälfte.
3. IP-Klassen notieren. 0 → A | 1 → B | 2 → C | ...
4. Kuchenstückgrösse Notieren: Wie viele Adressen haben in einem Subnetz platz? 0 → 256 | 1 → 128
5. Wie viele Kuchenstücke gibt es?

| Anzahl Bits | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| Dezimale Schreibweise | 0 | 128 | 192 | 224 | 240 | 248 | 252 | 254 | 255 |
| IP-Klasse | A | B | C | | | | | | |
| Kuchenstückgrösse | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Anz. Stücke | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 |

Hinweis: IP-Klassen werden heutzutage nicht mehr verwendet. Netzklassen sind unflexibel und wenig sparsam. Sie verwirren nur und werden in der Praxis nicht mehr eingesetzt. IP-Klassen wurden im Jahr 1993 per RFC 1518 und RFC 1519 durch das Classless Inter-Domain-Routing ersetzt. Bei CIDR werden innerhalb des gesamten Adressraumes Netze in flexiblen Grössen vergeben, folglich ist eine Ableitung der Netzgrösse aus der IP-Adresse nicht mehr möglich. Leider gib es immer noch Lehrer, die Netzklassen verwenden und unterrichten. Das ist sinnlos (BBZWITZ halt!!!).

## 1.11.2 Schritt 2: Rock the test!

1. **Alternative Schreibweise der Subnetzmask**e lässt sich mit Hilfe der Dezimalen Schreibweise und den Anzahl Bits ablesen.
2. Die **Klasse** kann man mit Hilfe der Dezimalen Schreibweise und der IP-Klasse ablesen. A geht von 0 bis (ohne mit) dort wo B anfängt.
3. Bei der **Anzahl mögliche Hosts im Subnetz:** $2^{\text{32-Alternative Schreibweise}}$ -2 oder $2^{\text{Anzahl Host-Bits}}$ -2. Das -2 kommt davon, weil man die Netz-ID und
4. **Anzahl mögliche Subnetze mit gleicher Maske**:
   $2^{\text{Wie viele Bits wurden zusätzlich zur Adressklasse gesetzt?}}$ (evtl. -2) oder $2^{\text{Anzahl Netzwerk Bits – Anzahl Bits der Klasse}}$ (evtl. -2)
   Das „evtl -2“ muss gemacht werden, weil dies der Lehrer so will. Dies hat man früher (vor unserer Geburt) so gemacht und vielleicht treffen wir mal so ein Router an...

5. **Netz-ID**: Wie gross ist die Kuchenstückgrösse? Dann rechnet man dort wo die Subnetzmaske ungerade wird die **IP-Adresse durch die Kuchenstückgrösse**. Dann **rechnet man ohne Rest zurück**. Dann hat man den Teil der Netz-ID. Man schreibt also dort wo die Subnetzmaske 255 ist das selbe wie bei der IP-Adresse hin. Dort wo die Subnetzmaske ungerade ist schreibt man das ausgerechnete hin und dort wo die Subnetzmaske 0 ist, schreibt man eine 0 hin.

6. **Broadcast-Adresse**: Man rechnet zur Netz-ID die Kuchenstückgrösse hinzu und erhält den Anfang vom nächsten Subnetz. Dann nimmt man 1 Bit weg. Also die grösste Adresse im ganzen Bereich.

7. **Host-ID**: Man rechnet den Teil der IP-Adresse (dort wo die Subnetzmaske ungerade ist) minus den „ungeraden“ Teil der Netz-ID. Dort wo die Subnetzmaske bei der IP-Adresse ungerade ist, übernimmt man genau das selbe. Der vordere Teil (also dort wo die Subnetzmaske gerade ist) lässt man einfach weg.

# 2 MRTG - Multi Router Traffic Grapher

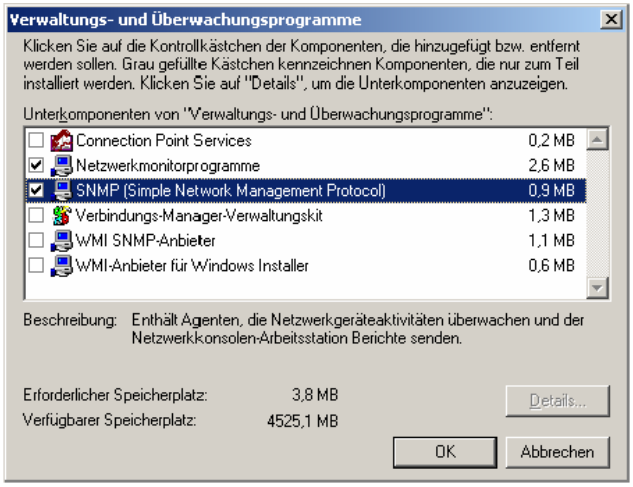
Ich ging dabei nach folgender Anleitung vor: http://oss.oetiker.ch/mrtg/doc/mrtg-nt-guide.en.html

## 2.1 Installation

### 2.1.1 Installation SNMP-Server

Wir installieren einen Windows Server 2003 und installieren dort den Webserver IIS und den SNMP-Server.

Wir installieren den SNMP-Dienst

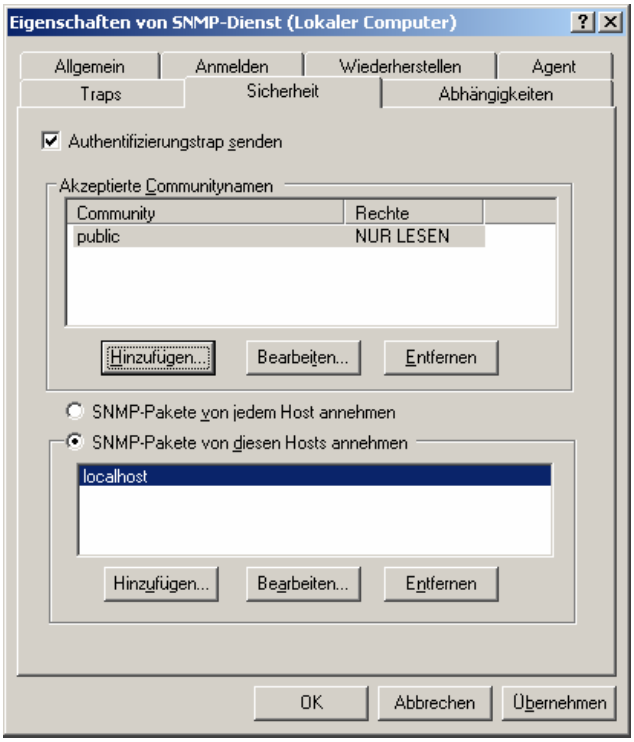



Standardmässig wird beim Windows Server 2003 keine Community gesetzt. Deshalb ist nach der installation noch kein Zugriff möglich. Diesen Zugriff müssen wir jetzt einrichten.

Dazu wechseln wir in die Eigenschaften des SNMP-Dienstes. Das finden wir in der Computerverwaltung unter der Kategorie Dienste.

Wir erstellen eine Community `public`, welche die Rechte `NUR LESEN` erhält.

SNMP-Pakete werden nur vom `Localhost` angenommen. Wenn weitere SNMP-Nachrichten angenommen werden sollen, dann müssen diese Hosts auch noch eingetragen werden.



### 2.1.2 Installation Active-Pearl

Wir laden die Software Active Perl herunter (http://www.activestate.com) und installieren diese. Perl ist nun aus der Kommandozeileneingabe bedienbar.

### 2.1.3 Installation MRTG

Die Software MRTG - Multi Router Traffic Grapher laden wir zuerst herunter http://oss.oetiker.ch/mrtg/

Das ZIP-Archiv wird direkt ins Root-Verzeichnis vom Laufwerk `C:\` entpackt. Hier finden wir also die MRTG-Software: c:\mrtg-2.16.2.

## 2.2 Konfiguration Windows Server 2003

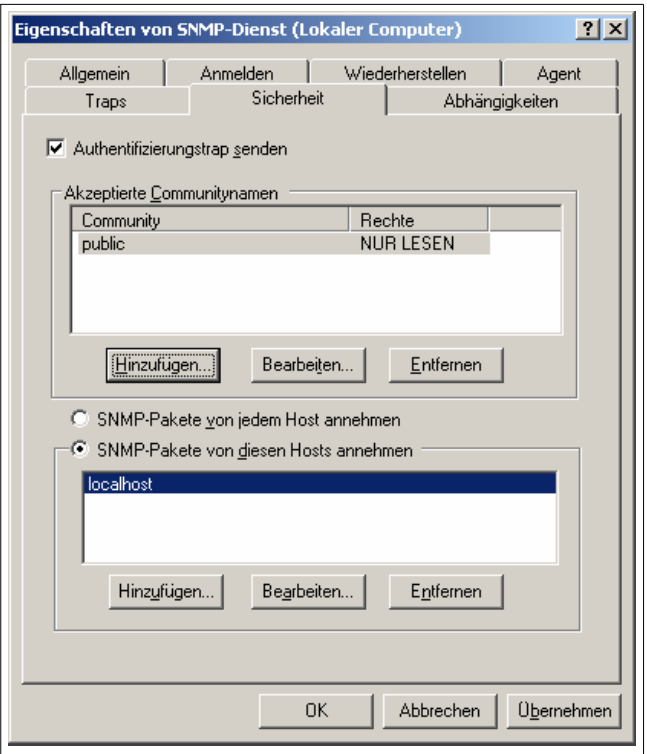
### 2.2.1 SNMP konfigurieren

Standardmässig wird beim Windows Server 2003 keine Community gesetzt. Deshalb ist nach der installation noch kein Zugriff möglich. Diesen Zugriff müssen wir jetzt einrichten.

Dazu wechseln wir in die Eigenschaften des SNMP-Dienstes. Das finden wir in der Computerverwaltung unter der Kategorie Dienste.

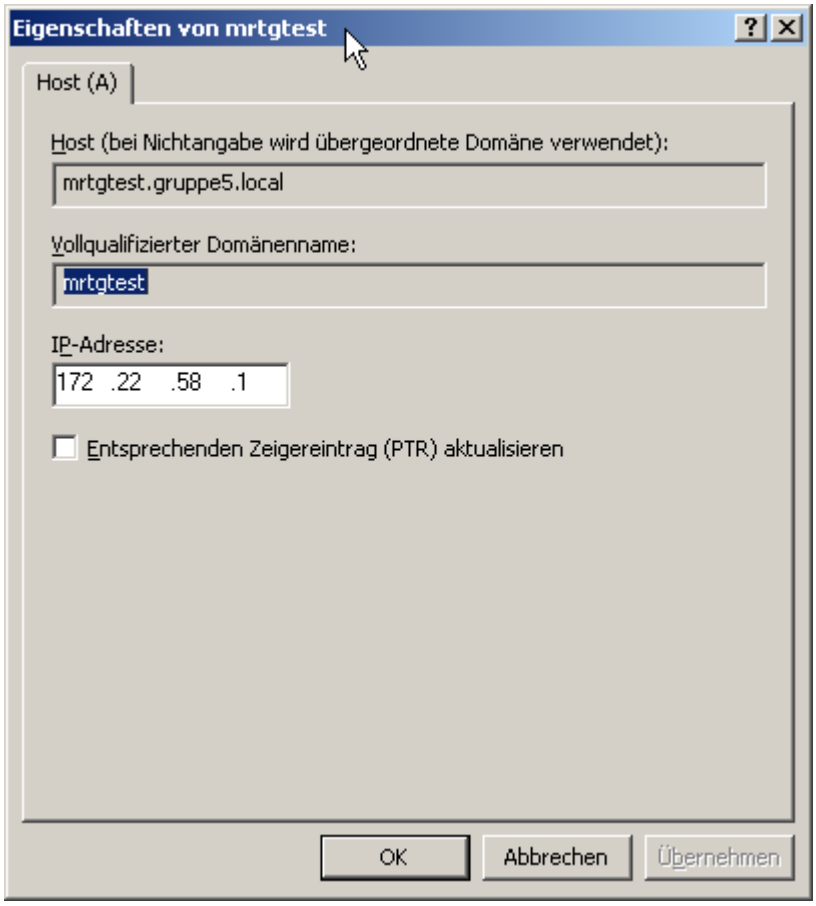
Wir erstellen eine Community `public`, welche die Rechte `NUR LESEN` erhält.

SNMP-Pakete werden nur vom `Localhost` angenommen. Wenn weitere SNMP-Nachrichten angenommen werden sollen, dann müssen diese Hosts auch noch eingetragen werden.




### 2.2.2 DNS-Eintrag erstellen

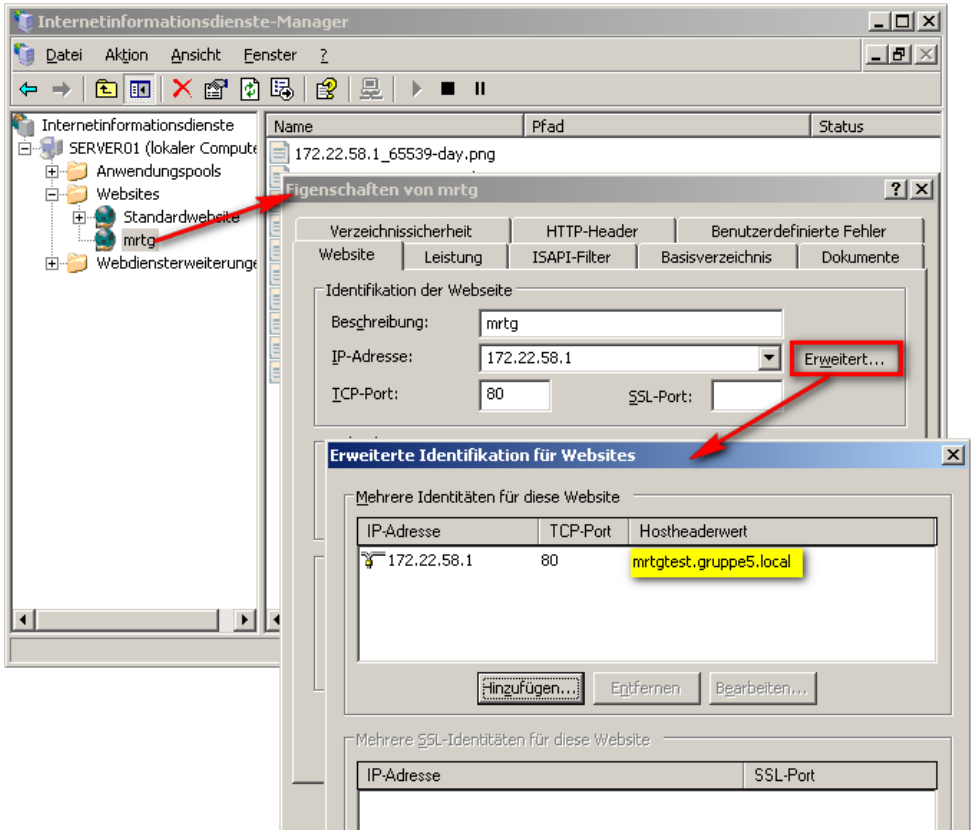
Wir erstellen einen DNS-Eintrag, damit man auf die Seite zugreifen kann.




### 2.2.3 IIS Konfigurieren

Beim IIS fügen wir eine neue Webseite hinzu.

Damit die Subdomain `mrtgtest` vom vom Webserver richtig intepretiert wird, müssen wir im IIS eine bestimmte Funktion aktivieren.




# 2.3 Konfiguration von MRTG

## Konfigfile erstellen

Wir erstellen ein Initiales MRTG-Configfile:

```
perl cfgmaker public@172.22.58.1 --global "WorkDir: c:\www\mrtg" --output
mrtg.cfg
```

## Konfigfile bearbeiten

Wir fügen `WorkDir: c:\www\mrtg` in den Anfang ein. Das ist das Root-Verzeichnis von der Website.

## MRTG testen

```
cd c:\mrtg-2.16.2\bin
perl mrtg mrtg.cfg
```

Die ersten zwei mal bekommen wir eine Fehlermeldung,die wir ignorieren. Diese Meldung kommt, weil noch kein Logfile vorhanden ist. Danach wird diese Meldung nicht mehr kommen.

Jetzt kann man alle paar Minuten dieses Kommando absetzen. Dann sehen wir schon den ersten Graph. Doch wir möchten das ja nicht manuell machen.

## MRTG als Dienst einrichten

Wir fügen `RunAsDaemon: yes` in das Konfigfile ein. Dann starten wir es mit

```
start /Dc:\mrtg-2.16.2\bin wperl mrtg --logging=eventlog mrtg.cfg
```

MRTG läuft nun immer im Hintergrund.

Wenn es Fehler gibt, kann man diese im Eventlog ansehen.

## MRTG beim anmelden automatisch Starten

Wir erstellen eine neue Verknüpfung.

- Ziel: `wperl mrtg --logging=eventlog mrtg.cfg`
- Starten in: `c:\mrtg-2.16.2\bin`

## Unser Konfigfile

## Andere Konfigurationen

Verlaufsrichtung der Grafik von rechts nach links einstellen:

```
Options[_]: growright, bits, avgpeak
```

Bit/sec statt Byte/Sec einstellen:

```
Options[_]: growright, bits, avgpeak
```

Durchschnitts-Spitzen anzeigen:

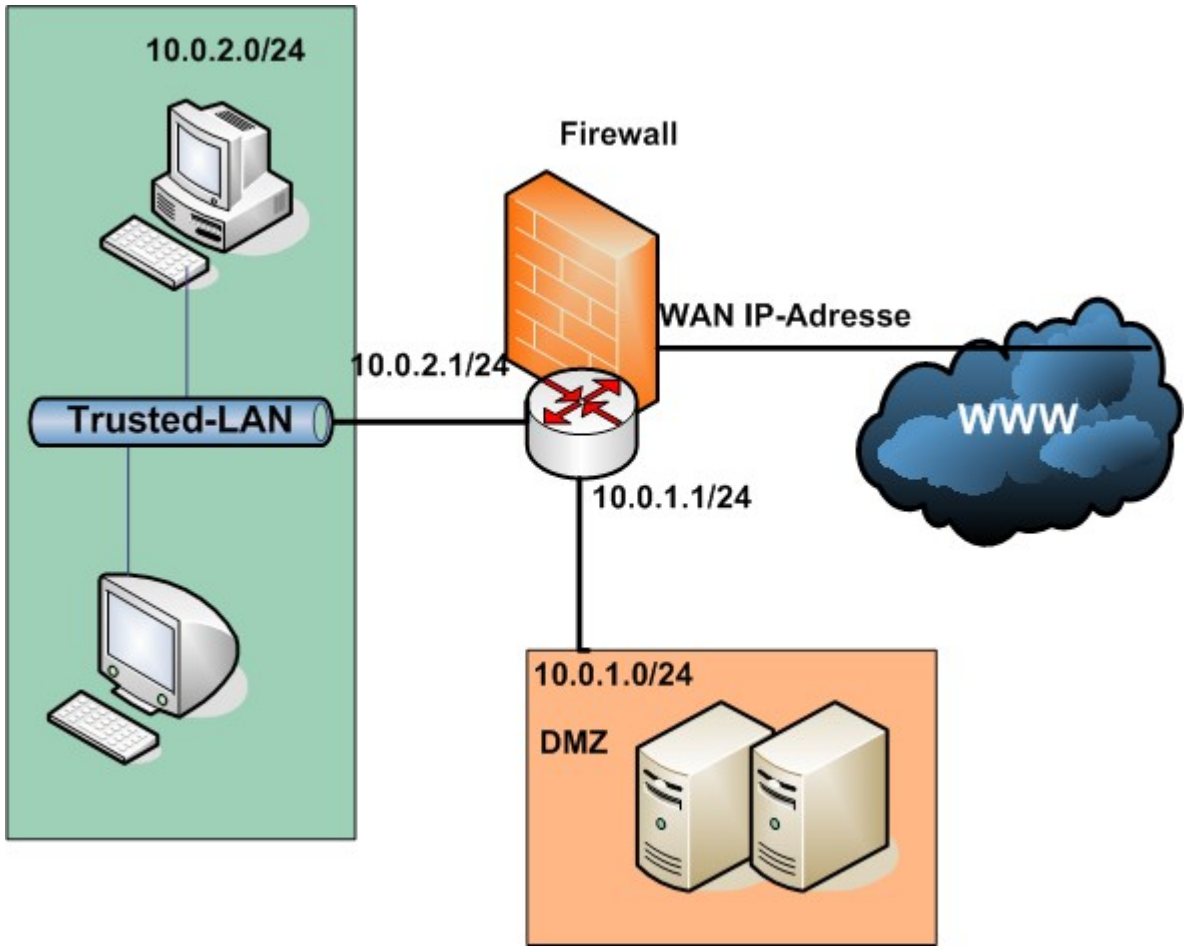
```
Options[_]: growright, bits, avgpeak
```

Spitzen anzeigen in Jahres-, Monats- und Wochenübersicht:

```
WithPeak[_]: ymw
```

# 3 Firewall

## 3.1 Netzwerkschema




## 3.2 Wie lautet die IP-Adresse von der Firewall?

Das ist oft die Frage, wenn es darum geht, ein Netzwerkgerät zu konfigurieren. Wir schliessen uns dazu an der ausgeschalteten Firewall an und lauschen mit Wireshark im promiscous-Mode auf eine Gratious-ARP-Nachricht beim Hochfahren des Gerätes:

```
    52 59.508057   Fortinet_72:09:63     Broadcast             ARP      Gratuitous ARP for 192.168.1.99 (Request)

⊞ Frame 47 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Fortinet_72:09:63 (00:09:0f:72:09:63), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Fortinet_72:09:63 (00:09:0f:72:09:63)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000000000
⊟ Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Fortinet_72:09:63 (00:09:0f:72:09:63)
    Sender IP address: 192.168.1.99 (192.168.1.99)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.99 (192.168.1.99)
```

# 3.3 Netzwerkkonfiguration

## Interfaces

Hier sehen wir schön auf einen Blick, wie wir die Konfiguration gemäss des Netzwerksplans erstellt haben:

| Name | IP / Netmask | Access | Status |
|---|---|---|---|
| **internal** | 10.0.2.1 / 255.255.255.0 | HTTPS,PING,SSH,HTTP | Bring Down |
| **modem** | / | | |
| **wan1** | 172.22.58.1 / 255.255.255.0 | PING | Bring Down |
| **wan2** | 10.0.1.1 / 255.255.255.0 | HTTPS,PING,SSH | Bring Down |

## Routen

| IP | Mask | Gateway | Device | Distance |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 172.22.58.254 | wan1 | 10 |

Und hier sehen wir die Routing-Tabelle der Firewall:

Die Default-Route erkennt man immer an `0.0.0.0/0.0.0.0`.

# 3.4 Firewallregeln erstellen

## Zugriffe

| | | | |
|---|---|---|---|
| Vom Spalte 1 in Ziel 1 | LAN | WAN1 (Internet) | WAN2 (DMZ) |
| LAN | - | Geschlossen: SSH | Offen: FTP, SMB |
| WAN1 (Internet) | Geschlossen: alles | - | Offen: FTP |
| WAN2 (DMZ) | Geschlossen: alles | Geschlossen: alles | - |

## VirtualIP

Wenn wir vom WAN1 her auf den FTP-Server zugreifen wollen, dann gehen wir auf die WAN1-IP-Adresse

vom Router. Woher weiss nun der Router, wohin er den FTP-Datenverkehr weiterleiten muss? Ich könnte ja mehrere Server in der DMZ stehen haben.

Dieses Problem kann man mit VirtualIPs lösen. Wir leiten die externe IP-Adresse von der Firewall direkt an den Server in der DMZ weiter:

| Name | IP | Service Port | Map to IP/IP Range | Map to Port |
|---|---|---|---|---|
| FTP-Server | wan1/172.22.58.1 | | 10.0.1.5 | |

Wenn man mehrere Server hätte, könnte man noch den nötigen Port angeben, damit die Firewall weiss, wohin die Datenpakete müssen (z.B. Port 21 > server01 und Port 80 > server02).

### Firewall Regeln

Hier sehen wir die Konfiguration:

| Status | ID | Source | Destination | Schedule | Service | Profile | Action |
|---|---|---|---|---|---|---|---|
| **internal -> wan1 (2)** | | | | | | | |
| ☑ | 4 | all | all | always | SSH | | DENY |
| ☑ | 1 | all | all | always | ANY | | ACCEPT |
| **internal -> wan2 (1)** | | | | | | | |
| ☑ | 6 | all | all | always | FTP<br>SAMBA | | ACCEPT |
| **wan1 -> wan2 (1)** | | | | | | | |
| ☑ | 8 | all | FTP-Server | always | FTP | | ACCEPT |
| **wan2 -> wan1 (1)** | | | | | | | |
| ☑ | 5 | all | all | always | ANY | | DENY |

## 3.5 Zugriff testen

Zum testen verwenden wir den OpenSource Portscanner `nmap`.

### IP- und Portscan vom WAN1 (Internet)

```
root@chaos:~#nmap -sP 172.22.58.0/24
Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-12 11:19 CET
Host 172.22.58.1 appears to be up.
MAC Address: 02:09:0F:72:09:67 (Unknown)
Host 172.22.58.23 appears to be up.
MAC Address: 00:17:31:4D:18:E9 (Asustek Computer)
Host 172.22.58.50 appears to be up.
Host 172.22.58.254 appears to be up.
MAC Address: 00:20:1A:20:06:10 (MRV Communications)
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.143 seconds
```

Wir sehen, welche Hosts online sind.

Dann machen wir einen Portscan auf die Firewall:

```
root@chaos:~#nmap 172.22.58.1
Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-12 11:20 CET
Interesting ports on 172.22.58.1:
Not shown: 1713 filtered ports
PORT    STATE  SERVICE
```

```
21/tcp  open   ftp
113/tcp closed auth
MAC Address: 02:09:0F:72:09:67 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.069 seconds
```

Wir sehen also, nur der FTP-Port (21) ist offen.

## Vom LAN ins WAN1 (Internet)

Hier wird der Zugriff vom User eingeschränkt. Er darf alles, ausser eine SSH-Verbindung herstellen. Er könnte sonst den ganzen Datenverker über SSH Tunneln und so gesperrte Seiten umgehen.

Wir machen einen Porscan auf einen SSH-Server:

```
root@chaos:~#nmap 172.22.58.50
Starting Nmap 4.62 ( http://nmap.org ) at 2009-03-12 11:26 CET
Interesting ports on 172.22.58.50:
Not shown: 1714 closed ports
PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.262 seconds
```

Der SSH-Server läuft also auf dem Server, jedoch sehen wir den Status gefiltert.

# 4 Squid-Proxyserver

## 4.1 Konfiguration Linux-Server

### 4.1.1 Benötigte Software installieren

Wir installieren den (Open)SSH-Server:

```
apt-get install ssh
```

Danach installieren wir Squid

```
apt-get install squid3
```

### 4.1.2 Konfiguration

#### Netzwerkkarte

Wir müssen noch die Netzwerkkarten konfigurieren:

```
debian@debian:~$cat /etc/network/interfaces
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
        address 172.22.58.10
        netmask 255.255.255.0
        network 172.22.58.0
        broadcast 172.22.58.255
        gateway 172.22.58.254
        dns-nameservers 172.20.10.20
        dns-search debian.local

iface eth1 inet static
      address 192.168.1.1
      netmask 255.255.255.0
      gateway 172.22.58.10

auto eth1
```

#### Squid-Konfiguration

Um die Kommentare zu entfernen, machen wir ein `grep` mt regulären Ausdrücken:

```
root@debian:~#cat /etc/squid3/squid.conf | grep ^[^#] >> /etc/squid3/squid.conf
```

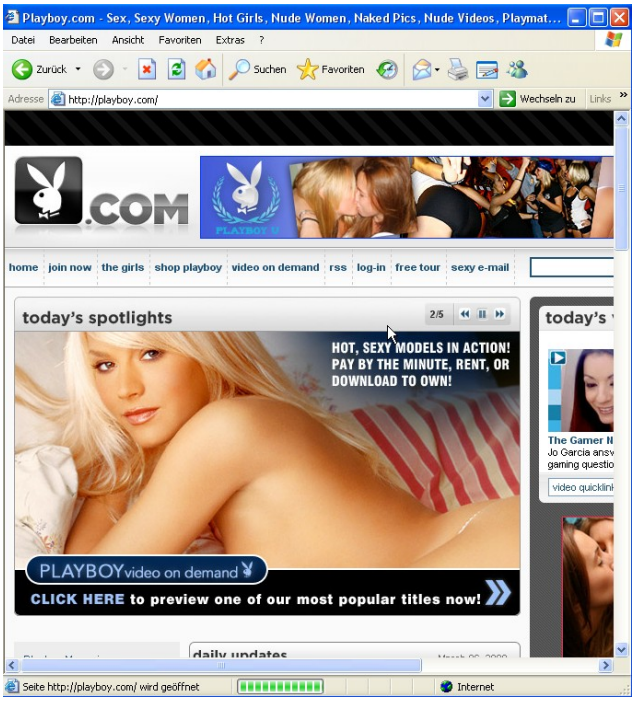
Danach passen wir das Konfigfile an. Das ist unter `/etc/squid3/squid.conf` zu finden.

```
debian@debian:~$cat /etc/squid3/squid.conf
# Diese Webseiten sind gesperrt
acl gesperrt dstdomain "/etc/squid3/domains.deny"
http_access deny gesperrt
acl gesperrt_reg url_regex -i "/etc/squid3/domains_reg.deny"
http_access deny gesperrt_reg
```

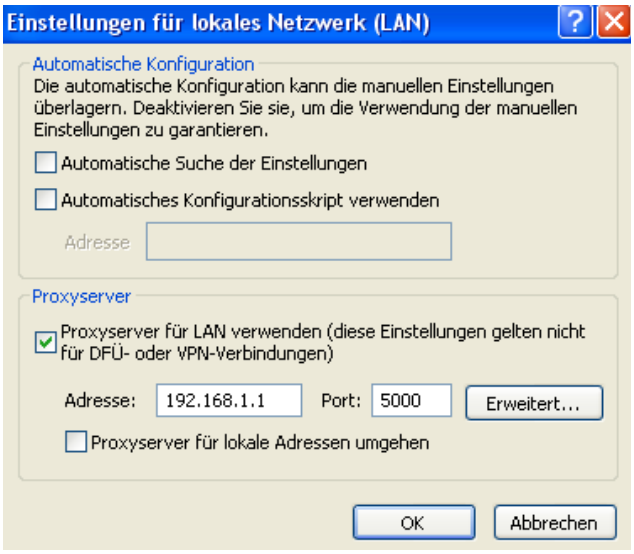
```
# Der PC des Admins darf auf die gesperrten Seiten zugreifen
acl adminpc src 192.168.1.10
http_access allow adminpc

acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8

acl localnet src 192.168.1.0/24

# Auf folgende Ports dÃ¼rfen zugegriffen werden
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

# Verweigere den Zugriff auf die anderen Ports
http_access deny !Safe_ports

http_access allow manager localhost
http_access deny manager
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access deny all

icp_access deny all

# Auf diesen Ports lÃ¤uft der Proxyserver
http_port 3128
http_port 5000
```

- In die Datei `domains.deny` fügen wir die verbotenen Seiten ein.
    - Diese Liste kann man natürlich vom Internet beziehen und über einen Cronjob automatisch auf den neusten Stand bringen.
- In die Datei `domains_reg.deny` fügen wir Reguläre Ausdrücke von verbotenen Wörtern ein. Dies bewirkt aber auch, wenn wir nach `Ans`**`porn`** suchen, dass dies gesperrt wird.

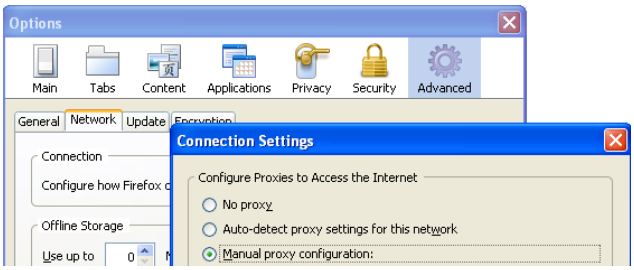
## 4.2 Konfiguration und Testen vom Client

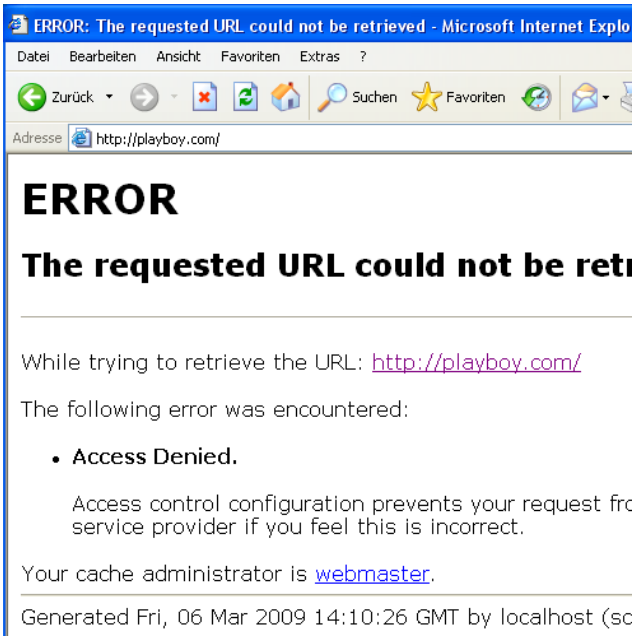



Momentan kann man noch auf Webseiten surfen, welche nur wenig mit der Arbeit zu tun haben:

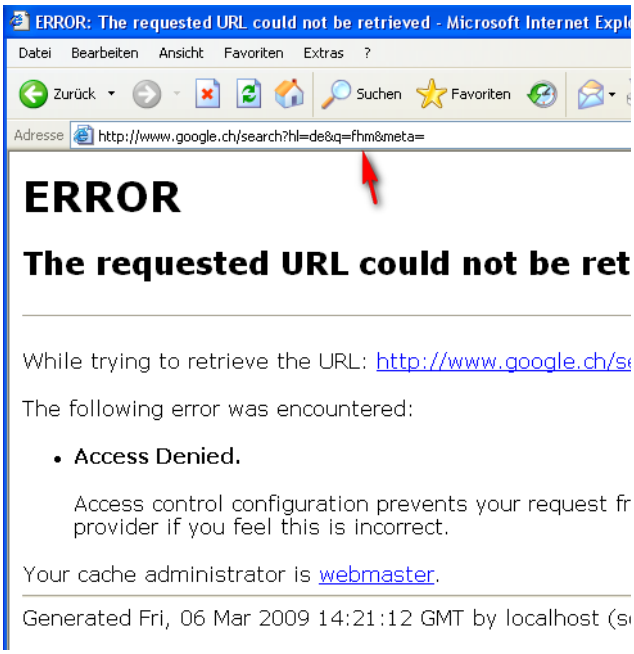



Beim Client tragen wir den Proxy-Server ein.



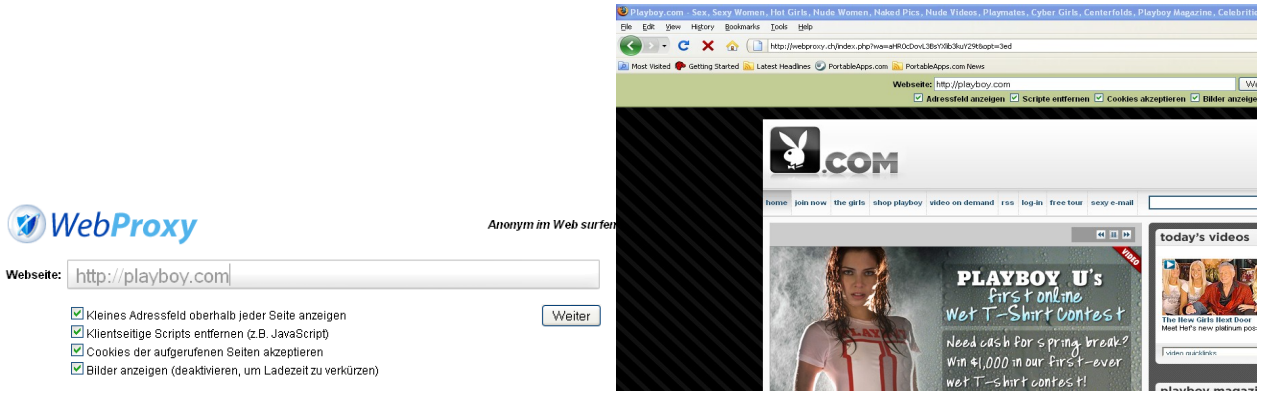

Playboy.com ist nun gesperrt.




Wenn das Stichwort FHM in der URL vorkommt, wir der Inhalt ebenfalls geblockt.

## 4.3 Umgehen der Websperre

Mit dem Dienst von `www.webproxy.ch` kann man den Proxy umgehen. Doch ich würde mich niemals ein Passwort von mir durch so einen Dienst jagen.




## 4.4 Transparenter Proxy

Neben dem üblichen Proxyeinsatz als Clientproxy, z.B. in lokalen Netzen, gibt es noch eine spezielle Form des Proxys, den so genannten transparenten Proxy oder reverse Proxy. Diese Anwendungsfälle unterscheiden sich im Wesentlichen dadurch vom normalen Proxy, dass sich dieser hier nicht direkt als Proxy zu erkennen gibt. Der Client merkt i.d.R. nicht, dass er einen Proxy nutzt und kann dessen Nutzung auch nicht verhindern. [23]

Der Proxyserver muss deshalb nicht auf jedem Client eingerichtet werden.

## 4.5 Auswertung der LogFiles

Das Logfile über verbotene Zugriffe befindet sich unter `/var/log/squid3/access.log`. Man kann manuell eine Überprüfung machen oder diverse Tools benutzen. Das sind zum Beispiel `squidview`, `sarg` oder `SRG`. Sarg und SRG erzeugen einen HTML-Report, den man auch gleich über ein Webserver auf dem Proxyserver ansehen kann.

### 4.5.1 Sarg

Wir installieren Sarg:

```
apt-get install sarg
```

Danach generieren wir ein Logfile:

```
sudo sarg -g e -o </pfad/zur/ausgabe>
```

Wir sehen die TOP 100 Sites, welche besucht wurden:

23 http://www.squid-handbuch.de/hb/node52_ct.html


Squid Analysis Report Generator

**Squid User Access Reports**

Period: -
Top 100 sites

| NUM | ACCESSED SITE | CONNECT | BYTES | TIME |
|---|---|---|---|---|
| 1 | playboy.com | 809 | 1.73M | 85.73K |
| 2 | www.fhm.com | 431 | 4.22M | 106.77K |
| 3 | www.playboy.com | 315 | 4.36M | 98.72K |
| 4 | www.fhm-online.de | 295 | 2.35M | 75.55K |
| 5 | feedroom.speedera.net | 115 | 311.75K | 15.79K |
| 6 | www.google.ch | 114 | 1.11M | 18.69K |
| 7 | tours.playboy.com | 110 | 651.55K | 24.62K |
| 8 | videoarticles.playboy.com | 100 | 1.38M | 41.13K |

Hier sehen wir auf einen Blick, welche Webseiten von einem User besucht werden:


Squid Analysis Report Generator

**Squid User Access Reports**

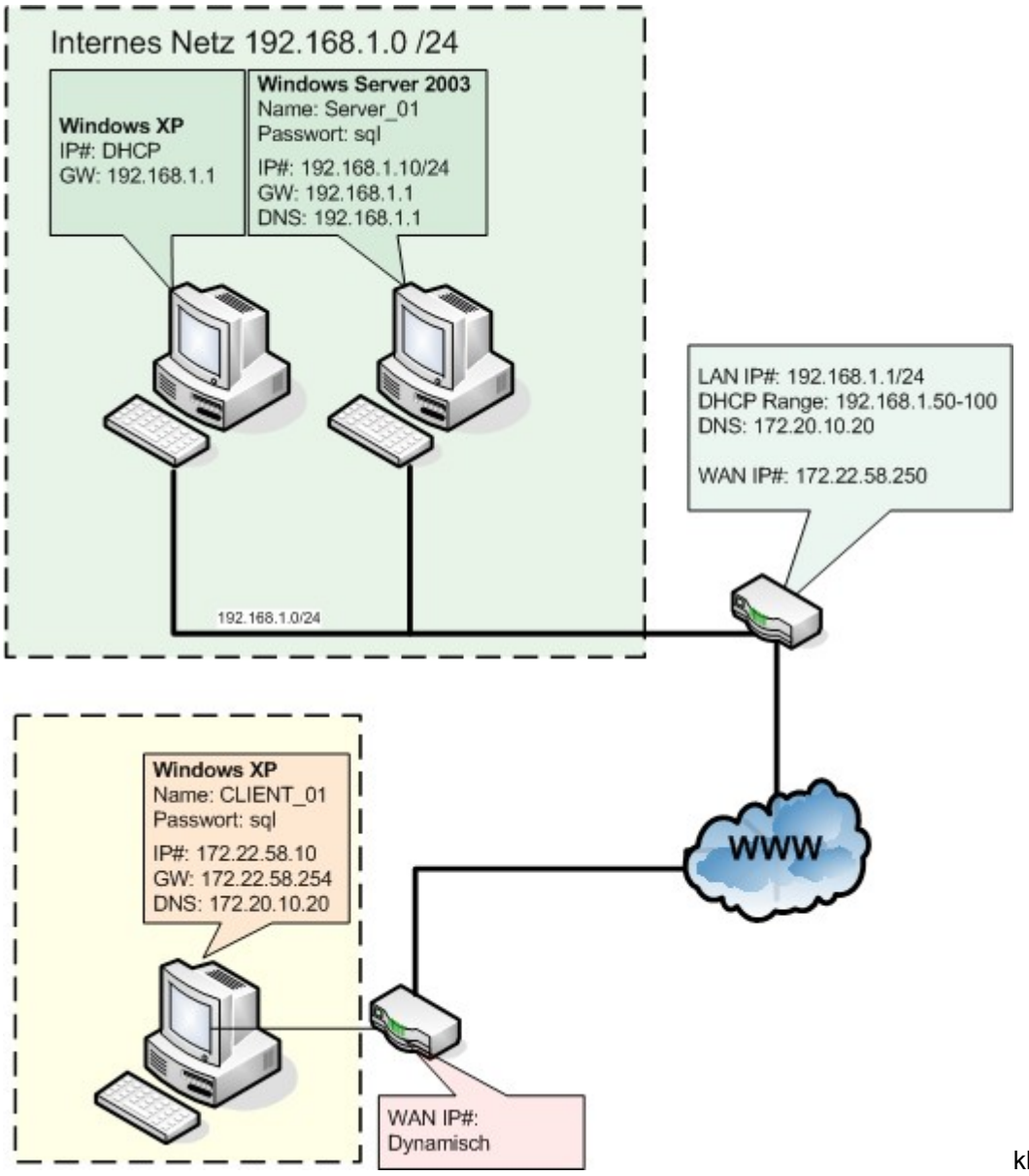
Period: -
User: 192.168.1.10
Sort: BYTES, reverse
User Report

| ACCESSED SITE | CONNECT | BYTES | %BYTES | IN-CACHE-OUT | | ELAPSED TIME | MILISEC | %TIME | |
|---|---|---|---|---|---|---|---|---|---|
| pbarticles1.wm.internapcdn.net | 20 | 33.17M | 34.61% | 0.00% | 100.00% | 00:05:14 | 314,544 | 16.07% | |
| brightcove.vo.llnwd.net | 14 | 16.93M | 17.67% | 0.00% | 100.00% | 00:01:00 | 60,964 | 3.11% | |
| v24.cache.googlevideo.com | 1 | 7.00M | 7.31% | 0.00% | 100.00% | 00:01:41 | 101,545 | 5.19% | |
| myvideo-840.vo.llnwd.net | 5 | 6.49M | 6.77% | 0.00% | 100.00% | 00:00:27 | 27,028 | 1.38% | |
| www.playboy.com | 315 | 4.36M | 4.55% | 0.49% | 99.51% | 00:01:38 | 98,726 | 5.04% | DENIED |
| www.fhm.com | 431 | 4.22M | 4.41% | 0.96% | 99.04% | 00:01:46 | 106,777 | 5.46% | DENIED |
| a399.v9191b.c9191.g.vm.akamaistream.net | 10 | 2.92M | 3.05% | 0.00% | 100.00% | 00:00:13 | 13,095 | 0.67% | |
| www.fhm-online.de | 295 | 2.35M | 2.46% | 0.32% | 99.68% | 00:01:15 | 75,554 | 3.86% | DENIED |
| fpdownload2.macromedia.com | 3 | 1.88M | 1.97% | 0.00% | 100.00% | 00:00:52 | 52,427 | 2.68% | |
| playboy.com | 809 | 1.73M | 1.82% | 10.18% | 89.82% | 00:01:25 | 85,732 | 4.38% | DENIED |
| admin.brightcove.com | 36 | 1.56M | 1.63% | 0.27% | 99.73% | 00:00:28 | 28,509 | 1.46% | |
| videoarticles.playboy.com | 100 | 1.38M | 1.45% | 0.03% | 99.97% | 00:00:41 | 41,139 | 2.10% | |
| www.google.ch | 114 | 1.11M | 1.17% | 6.06% | 93.94% | 00:00:18 | 18,693 | 0.96% | |
| www.playboystore.com | 75 | 950.41K | 0.99% | 0.74% | 99.26% | 00:00:26 | 26,704 | 1.36% | |
| tours.playboy.com | 110 | 651.55K | 0.68% | 2.35% | 97.65% | 00:00:24 | 24,625 | 1.26% | |
| mail.google.com:443 | 25 | 636.11K | 0.66% | 0.00% | 100.00% | 00:00:35 | 35,265 | 1.80% | |

# 5 Virtual Private Network

## 5.1 Netzwerkschema

Wir bauen unser Netzwerk folgendermassen auf:




klökl

## 5.2 Konfiguration auf dem VPN-Gateway

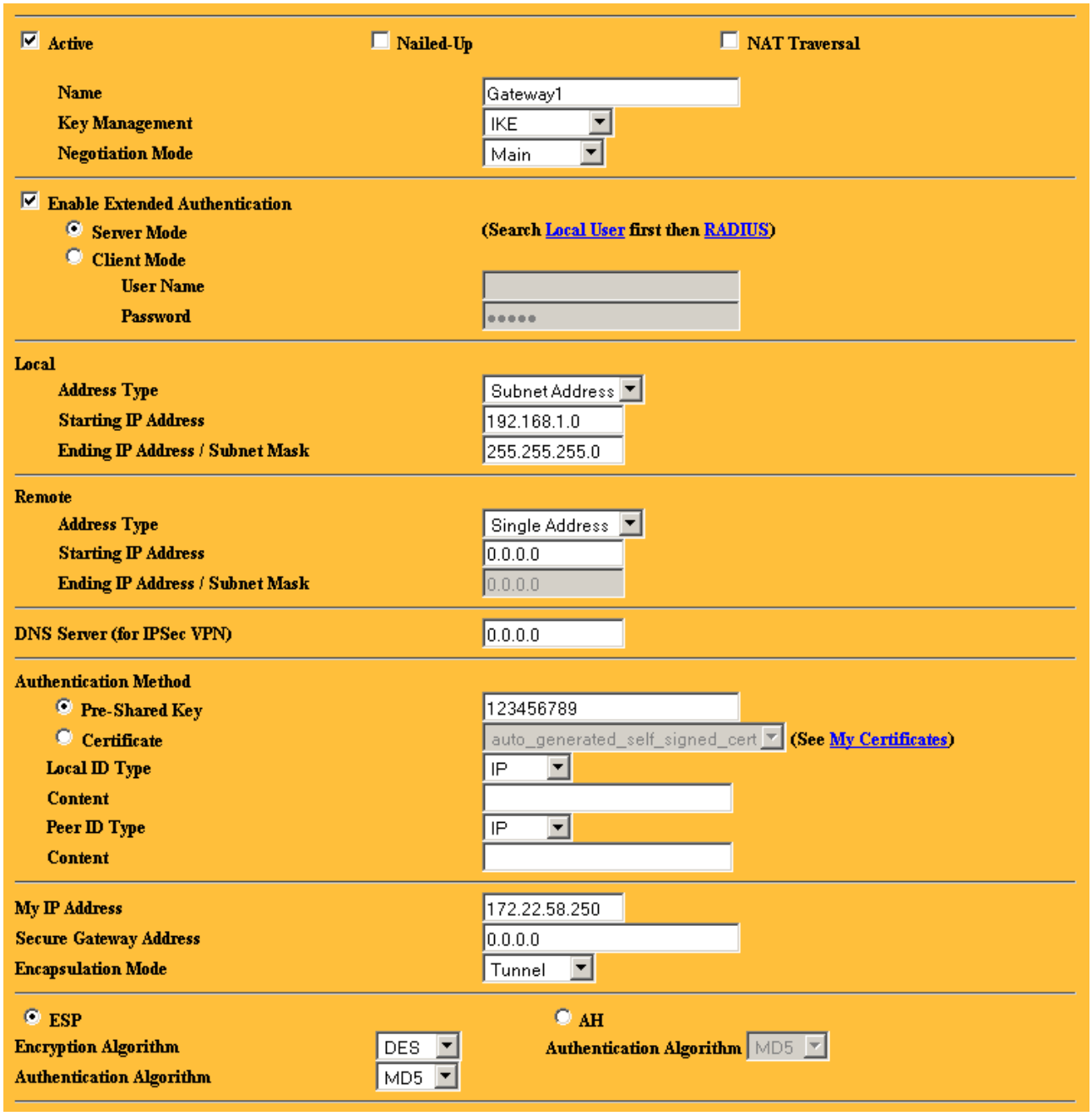
Wir nutzen eine ZyWall um den VPN-Zugang zu realisieren.

### IP-Einstellungen

- LAN IP-Adresse: 192.168.1.1 /24

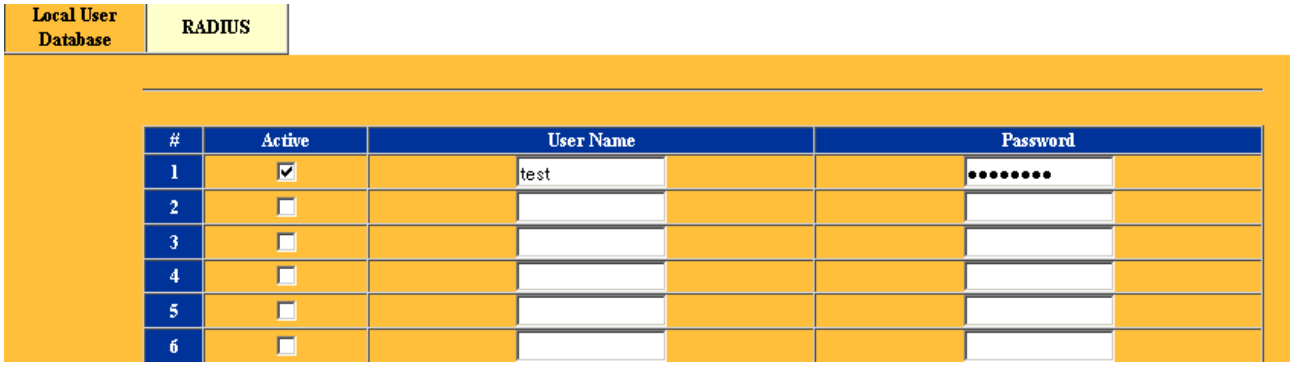
- WAN IP-Adresse: 172.22.58.250 /24
- DNS-Server: 172.20.10.20
- Default Gateway: 172.22.58.254

## VPN-Einstellungen




## Auth. Server

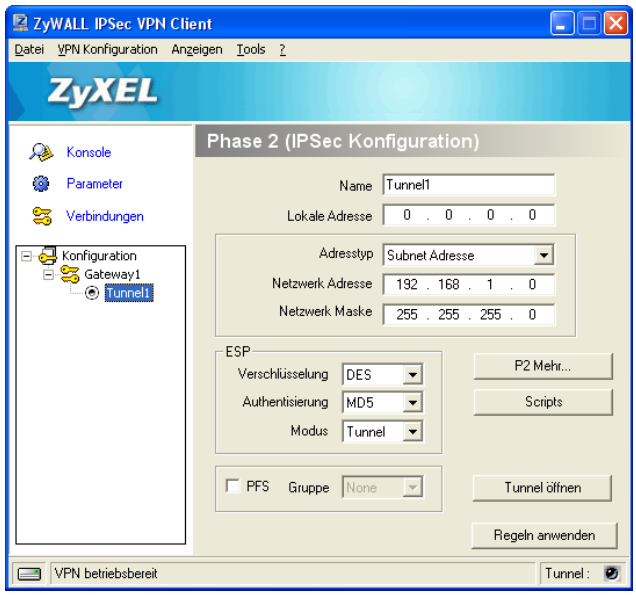
Hier kann man den Username und das Passwort eintragen, mit dem sich danach der User authentifizieren kann.



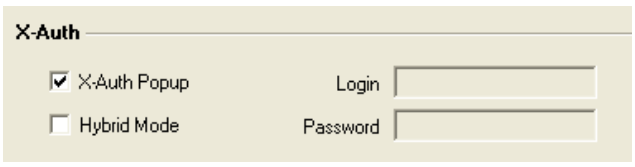

## 5.2.1 Konfiguration Client


Wir erstellen eine neue Phase 1. Das ist die Authentisierung.

Der IPSec Gateway ist die WAN-IP-Adresse von der Zywall.



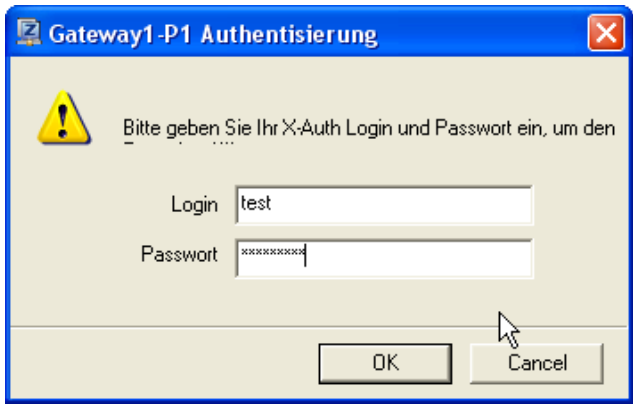

Wir geben das Subnetz an, in das wir nachher eingeschleust werden wollen.




Wir müssen bei `mehr Parameter ...` X-Auth Popup eingeben, damit sich der User danach authentifizieren kann.

Dabei verweist er auf die interne Datenbank der ZyWall.

Jetzt können wir die Verbindung aufbauen.




## 5.2.2 Wie funktioniert die Kommunikation?

Erreiche ich den Server?

```
C:\>ping server01

Ping server01 [192.168.1.10] mit 32 Bytes Daten:

Antwort von 192.168.1.10: Bytes=32 Zeit=1ms TTL=127
Antwort von 192.168.1.10: Bytes=32 Zeit=1ms TTL=127

Ping-Statistik für 192.168.1.10:
    Pakete: Gesendet = 2, Empfangen = 2, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
STRG-C
^C
C:\>
```

OK. Der Server kann ich über `server01` erreichen.

Wir sehen uns mal unsere IP-Adresse an:

```
C:\>ipconfig

Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 172.22.58.10
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 172.22.58.254
C:\>
```

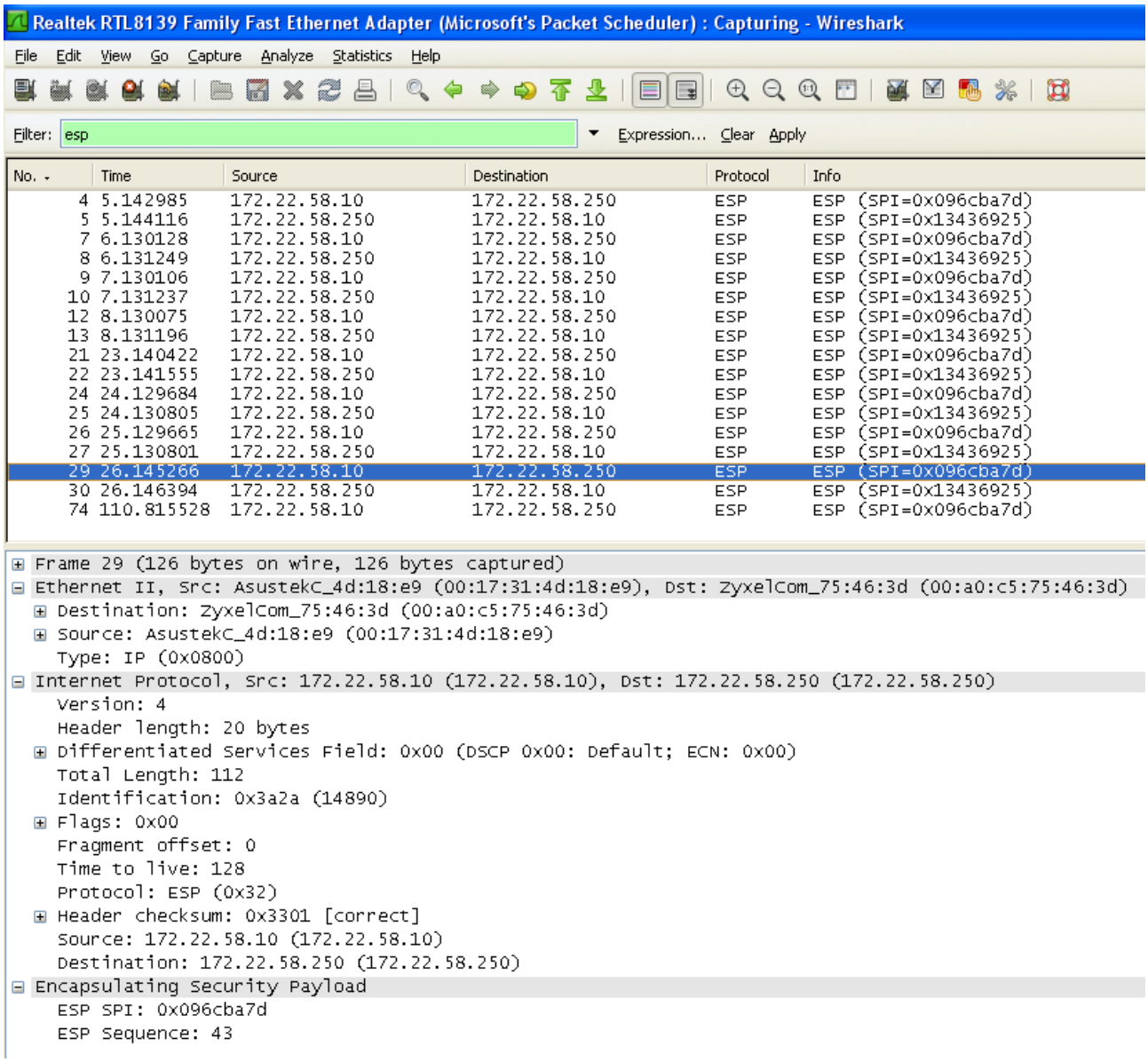
Ich habe also immer noch die selbe IP-Adresse wie vorher.

Wie wird das IP-Paket an den VPN-Gateway weitergeleitet? Ich erwarte nun in der Routing-Tabelle einen neuen Eintrag. Wir schauen mal die Routing-Tabelle an:

```
C:\>netstat -r

Routingtabelle
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 17 31 4d 18 e9 ...... Realtek RTL8139-Familie-PCI-Fast Ethernet-NIC -
Paketplaner-Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0    172.22.58.254    172.22.58.10       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      172.22.58.0    255.255.255.0     172.22.58.10    172.22.58.10       20
     172.22.58.10  255.255.255.255        127.0.0.1       127.0.0.1       20
   172.22.255.255  255.255.255.255     172.22.58.10    172.22.58.10       20
        224.0.0.0        240.0.0.0     172.22.58.10    172.22.58.10       20
  255.255.255.255  255.255.255.255     172.22.58.10    172.22.58.10       1
Standardgateway:     172.22.58.254
===========================================================================
Ständige Routen:
  Keine
C:\>
```

Kein Eintrag für das Netz `192.168.1.0 /24`. Doch an welche IP-Adresse wird das IP-Paket weitergeleitet?

Laut der Routing-Tabelle wird da IP-Paket an den Standardgateway `172.22.58.254` weitergeleitet. Doch der weiss gar nichts vom VPN. Das VPN-Paket muss also an ein anderen Ort weitergeleitet werden. Wir schauen mal mit Wireshark hinein:




Et voilà: Wir sehen, dass der Client `172.22.58.10` das IP-Paket an die WAN IP-Adresse `172.22.58.250` vom VPN-Gateway schickt.

Das erscheint mir sehr urchig. Ich verstehe nicht wieso das so funktioniert. Das wird wohl irgendwie intern gehandhabt.

## 5.2.3 Informationen

### Phase 1 und Phase 2

Phase 1: Austausch über den Verbindungsaufbau (Verschlüsselungstyp, Algorithmus)

Phase 2: Logininformationen

### 5.2.4 Verschlüsselungsalgorithmen

#### DES

- symmetrischer Verschlüsselungsalgorithmus
- 56 Bit lang
- Heute kaum verwendet, da unsicher

#### 3DES

- Dreifachverschlüsselung mit drei unabhängigen, voneinander verschiedenen Schlüsseln
- 168 Bits
- Sicher
- Durch Dreifachverschlüsslung langsam

#### MD5

- Message Digest Algorithm
- kryptographische Hashfunktion
- 128-Bit
- 1991 von Ronald L. Rivest

#### SHA1

- secure hash algorithm 1
- kryptographische Hashfunktion
- Berechnung eines eindeutigen Prüfwerts
- im Sommer 2006 wurde eine wesentliche Schwäche dieses Algorithmus entdeckt

#### AES

- Nachfolger von DES
- im Oktober 2000 als Standard definiert
- variable Schlüssellänge von 128, 192 oder 256 Bit

# 6 OpenWRT

## 6.1 Was ist OpenWRT?

OpenWrt ist ein Embedded Linux, das insbesondere für Router konzipiert wurde. Es wird häufig eingesetzt und ersetzt die vorinstallierte Firmware des Herstellers. Im Gegensatz zu einer statischen Firmware setzt OpenWRT auf ein voll beschreibbares Dateisystem sowie einen Paketmanager und ermöglicht es somit, einen WLAN-Router flexibel um ursprünglich nicht vom Hersteller vorgesehene Funktionen zu erweitern.[24]

### Entstehung

Im Juni 2003 stellten Andrew Miklas und weitere Programmierer fest, dass die Firma Linksys in ihrer Produktserie WRT54G den unter den Bestimmungen der GNU General Public License (GPL) veröffentlichten Quelltext des Linux-Kernels und anderer Software verwendete, ohne jedoch ihren modifizierten Quelltext der Allgemeinheit zur Verfügung zu stellen, wie es von der GPL verlangt wird.[2] Nach einem mehrere Monate andauernden öffentlichen Appell an Linksys lenkte die Firma schließlich größtenteils ein und veröffentlichte im Oktober 2003 fast den gesamten modifizierten Quelltext des WRT54G-Linuxkernels, bis auf den Treiber für den in dieser Routerserie verbauten Broadcom WLAN-Chipsatz.[3] Um den Druck auf Linksys und andere Routerhersteller zu erhöhen, gründete Harald Welte, der Hauptentwickler des Linux-Netzwerkmoduls netfilter/iptables, infolgedessen die Initiative gpl-violations.org.[4] Dadurch wurde es möglich, die von Linksys und später anderen Firmen veröffentlichte Software zu modifizieren und somit den Wünschen der Benutzer entsprechend anzupassen.

## 6.2 Was wir machten

Wir hatten einen Linksys wrt54g Router:


Wir probierten diverse WRT-Devirate auss.

24 http://de.wikipedia.org/wiki/OpenWrt

- OpenWRT
- DD-WRT
- Tomato
- Hyper-WRT

Die Vorteile des WRT54GL liegen auf der Hand: Viele freie Programmierer erweitern die Firmware freiwillig in ihrer Freizeit und packen neue Funktionen ein. Mit der Zeit kommen sogar Funktionen hinzu, die sonst nur auf sehr teurer Netzwerkhardware verfügbar wäre.

Wir versuchen nun, die Firmwares vollkommen auszukosten. Es soll möglich sein einen Content-Filter zu konfigurieren, Transparent-Proxy einzustellen und Access Restrictions zu definieren.

### 6.2.1 Feststellung im Vergleich zu teuren Geräten

Wir haben festgestellt, dass viele Firmwares einiges können, jedoch überzeugt hat uns keine vollkommen. Vielen teuren Geräten kann der WRT sicherlich den Rang ablaufen aber in der Spitzenklasse, wo Cisco Geräte im Vergleich stehen, kann man mit dem WRT nicht mithalten.

# 7 Mein persönlicher Kursrückblick

## 7.1 Positives

- Die Kursunterlagen wurden schön gedruckt und geringelt abgegeben (obwohl nicht doppelseitig...)
- Sehr gut, dass etwas mit Linux angeboten wird.
- Der Kursleiter konnte kompetente Antworten geben, falls wir etwas wissen wollten.
- Ich durfte meine Kursdokumentation in OpenOffice.org schreiben.
- Ich durfte meinen EEEPC einsetzen.
- Wir durften den OpenWRT-Router von Semir einsetzen und somit ein Zusatzprogramm machen.

## 7.2 Negatives

- Am Anfang mussten wir nur viel Theorie im Internet lesen. Dies ist schade, denn wir haben nicht viel Zeit im Kurs. Da sollte man die Zeit anders einsetzen.
- Wir müssen wie jedes mal die Pcs selber von Hand installieren. Dies ist verlorene Zeit! Danach müssen alle Treiber installiert werden und zusätzliche Programme wie z.B. Den Adobe Reader etc... Wenn man den PC über ein Image installieren würde, würde das die Arbeit sehr erleichtern.
- Auch die benötigte Software sollte zentral gespeichert werden. Wenn jeder jedes Programm vom Internet herunterladen muss, braucht es viel zu viel Zeit. Die Infrastruktur vom VFI sollte ja eigentlich ein Vorbild für uns sein. Z.B. Zentrale Datenhaltung, Images.
- Ich persönlich finde die Kursunterlagen schrecklich, weil:
  - Viele Links funktionieren nicht mehr
  - Die Nummerierung ist unlogisch. z.B. geht's von 6.3 direkt zu 6.3.1.1
  - Die Gliederung / Strukturierung ist nicht durchdacht. Mehrmals müssen wir beschreiben was eine Firewall ist, was sie macht und wie sie arbeitet.
  - Ich denke der Ersteller weiss selber nicht mehr, wie die Unterlagen strukturiert sind.
  - Bei kopierten Texten, Bildern, etc. fehlen die Quellenangaben!!!
  - Texte wurden unschön vom Internet her kopiert / übernommen (Formatierung...)
  - Es steht bei Hilfsmittel: Ihre Schulunterlagen. Welche Schulunterlagen???
- Sehr schade, dass kein Linux-Wissen vermittelt wird!
- Wir bekamen nie während dem Kurs eine Rückmeldung über unsere bereits erstellte Arbeit (Dokumentation, Arbeitsweise, sozialer Umgang, etc...)
- Wir hatten nie kleine Unterrichtseinheiten während dem Kurs. Das hat mir bis jetzt immer gefallen während den Kursen.
- Es wurden zu wenig Firewalls organisiert. 6 Gruppen in 5 Arbeitstagen braucht mehr als 5 Firewalls.

## 7.3 Sonstiges

- Eigentlich wollte ich meine Kursdoku in LaTeX schreiben, doch dazu kam es leider nicht. Ich blieb bei OpenOffice.org... Hoffendlich wird sich das ein anderes mal ergeben!

# 8 Glossar

| | |
|---|---|

# 9 Gute Links

- VPN: http://www.virenschutz.info

# Stichwortverzeichnis