

KLAUS DEMBOWSKI

Lokale Netze

Handbuch der kompletten Netzwerktechnik

16 LAN-Sicherheit

Durch die meist standardmäßige Verbindung mit dem Internet ist auch ein lokales Netzwerk insbesondere durch den Angriff von außen bedroht. Sicherheitshinweise und -tipps zu WLANs sowie Switches und Routers lassen sich in den jeweiligen Kapiteln finden, während es hier vorwiegend um grundlegende Dinge zur LAN-Sicherheit gehen soll.

16.1 Gefahren und Sicherheitsmaßnahmen

Die Risiken oder Gefahren, die sich durch den Einsatz von Computern und Netzwerken ergeben, sind vielfältiger Art. Hier geht es allein um die Gefahren, die unmittelbar durch die Benutzung von Computernetzwerken auftreten können.

In Firmen ist das größte Gefahrenpotential durch Irrtum und Nachlässigkeit der eigenen Mitarbeiter gegeben. An zweiter Stelle findet sich bereits die Bedrohung durch Schadprogramme.

Gefahrenbereich	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51 %
Malware (Viren, Würmer, Trojanische Pferde usw.)	2	1,34	1	2,80	1	54 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9 %
Softwaremängel/-defekte	4	0,57	5	0,96	3	43 %
Hacking (Vandalismus, Probing, Missbrauch usw.)	5	0,48	3	1,26	5	9 %
Hardwaremängel/-defekte	6	0,40	8	0,32	4	38 %
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15 %
höhere Gewalt (Feuer, Wasser usw.)	8	0,24	11	0,04	9	8 %
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8 %
Mängel der Dokumentation	10	0,15	10	0,20	6	17 %
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8 %
Sonstiges	12	0,03	12	0,00	12	3 %

Quelle: kes/Microsoft

Abbildung 16.1: Die Gefahrenbereiche in deutschen Firmen

Bis Mitte des Jahres 2004 waren rund 100.000 unterschiedliche Computer-Viren im Umlauf, und jeden Monat entstehen hunderte von neuen. Diese haben bislang weltweit Kosten und Schäden in Milliardenhöhe verursacht. Allein in Deutschland ist jährlich von einer dreistelligen Millionensumme mit steigender Tendenz auszugehen.

Die Motivation für die Erstellung von Schädlingen ist unterschiedlich, wobei den als Hacker, Cracker und Scriptkids bezeichneten Experten jedoch gemein ist, dass sie sich für Daten auf fremden Computern interessieren. Hacker und Cracker verfügen über sehr viel technisches Know-how und sind auf ihren jeweiligen Gebieten ausgesprochene Spezialisten. Hacker sind meist aus »Sportgeist« aktiv, während Cracker sich bereichern wollen. Scriptkids probieren – nicht selten im kriminellen Auftrag – fertige Hackerprogramme (Scripts) aus, so dass hier nicht unbedingt Spezialisten am Werke sind, was jedoch nicht bedeutet, dass ihre Aktivitäten keine gravierenden Auswirkungen haben. Vielmehr hat gerade diese Schadsoftware in den letzten Jahren die größte Verbreitung gefunden und wahrscheinlich auch den größten Schaden verursacht. Weil die Scriptkids vielfach noch nicht im vollen Umfang strafmündig sind, werden ihre Dienste auch gern von Kriminellen in Anspruch genommen, wobei sie nicht selten in Chaträumen oder Diskussionsforen um entsprechende »Gefälligkeiten« gebeten werden.

Angaben zu finanziellen Schäden, die durch derartige Software (Malware) entstanden ist, sind nicht einfach zu ermitteln, zumal geschädigte Firmen den Befall als Imageschaden ansehen und ihn deshalb nicht veröffentlichen. Daher entsprechen die offiziellen Angaben zum Befall mit Schadsoftware und deren hervorgerufene Schäden auch vermutlich nicht der Wirklichkeit, die Dunkelziffer ist weitaus höher.

Selbst ein recht unerfahrener Computeranwender findet im Internet die passenden Werkzeuge (Toolkits) für die Erstellung von Schadsoftware. Dies sind dann zwar nur Abwandlungen von bereits bekannten Viren und Würmern, so dass die aktuelle Antivirussoftware anhand der jeweiligen Signatur diese als solche erkennen kann. Allerdings führt die individuelle Kombination einzelner Codesequenzen mit bestimmten Dateitypen (*.com, *.doc) sowie unterschiedlichen Verteilungswegen (Mail, Internet) immer wieder dazu, dass sie dennoch den Weg zum Anwender finden und diverse Manipulationen ausführen können. Dazu gehört es auch, PCs zu »kapern«, um dann mit möglichst vielen Computern ein so genanntes Bot-Netz aufzubauen. So wird der (unfreiwillige) Zusammenschluss von Computern bezeichnet, mit deren Hilfe dann SPAM (siehe Kapitel 16.1.5) verteilt oder auch gezielte Angriffe (Distributed Denial of Service) gegen bestimmte Firmen oder Institutionen ausgeführt werden. Der Aufbau von Bot-Netzen ist ein lohnendes Geschäft, denn diese werden an entsprechende (kriminelle) Interessenten vermietet, was laut Meldung des Heiseverlages pro Stunde ca. 80 € oder auch 22000 € pro Monat kostet.



Bei gekaperten PCs werden verschiedene TCP/IP-Funktionen aufgerufen, was an offenen Ports (Anzeige mit netstat -a) zu erkennen ist, die nicht wieder automatisch geschlossen werden. Im IPv6-Stack sind hierfür entsprechende Sicherheitsmaßnahmen implementiert.

Die Gefahr, die von einem PC ausgeht, der nicht mehr der eigenen, sondern einer ferngesteuerten Kontrolle unterliegt, ist deshalb kaum abzuschätzen, weil der »momentane Inhaber« ihn aus Ausgangspunkt für das weitere Verteilen von Schadsoftware, von rechtsextremen oder auch pornografischen Inhalten sowie das Plündern von Bankkonten einsetzen kann, wobei das eigene LAN als Ausgangspunkt des Übels festgestellt werden kann.

Der eigentliche PC-Besitzer, der nichts von alledem weiß, sieht sich dann zunächst dem Verdacht ausgesetzt, dass er selbst diese Taten begangen hätte, was strafrechtliche und zivilrechtliche Folgen sowie finanzielle Ansprüche der Geschädigten mit sich bringen kann.

Die Rechtssprechung deshalb ist in derartigen Fällen bereits dazu übergegangen, dem wirklichen Benutzer des Computer zumindest eine Fahrlässigkeit, mitunter sogar eine Teilschuld zu attestieren, wenn er nicht die bekannten Sicherheitsmaßnahmen wie Virens Scanner und eine Firewall zur Absicherung eingesetzt hat. In mehreren Urteilen haben Gerichte derartige Entscheidungen damit begründet, dass man bei Leuten, die mit PCs arbeiten, davon ausgehen kann, dass sie über die Gefahren hinsichtlich der Datensicherheit, wozu auch die Datensicherung gehört (Backup), hinlänglich informiert sind. Woher sie diese Informationen erhalten, ob sie sich diese privat aneignen, wovon ausgegangen wird, wenn sie auch privat einen PC nutzen, oder ob der Arbeitgeber entsprechende Schulungen vorsieht, ist dabei nicht von Bedeutung.


Gegen die bisher erwähnten Gefahren gibt es entsprechende Abhilfe in Form von Antivirus- und Antispy-Software. Wohingegen es jedoch keinen direkten Schutz gibt, ist die (vermeintliche) Ahnungslosigkeit der Anwender, die Mails unbekannter Herkunft und deren Anhänge öffnen und dann auch auf Phishing hereinfliegen. Grundsätzlich sollten keine Anhänge unbekannter Emails geöffnet werden, und ein Virens Scanner sollte stets im Hintergrund laufen.

Mit Phishing wird dem Anwender eine seriöse Internet-Seite wie von einer Bank oder einem Auktionshaus vorgegaukelt, die angeblich wichtige Informationen enthält und an irgendeiner Stelle seine Kontonummer, die PIN oder die TAN verlangt. Mit diesen Informationen kann der Angreifer dann per Online-Banking Beträge vom Konto des Ahnungslosen abbuchen. In der ersten Jahreshälfte 2006 wurden mehr als 157000 Phishing Mails versendet, und es ist davon auszugehen, dass eine ganze Reihe von Leuten wieder darauf reingefallen sind, zumal der geprellte Kunde bei der Bank beweisen muss, dass er nicht der Abbucher war, was meist auf eine langwierige Auseinandersetzung hinausläuft.

Während ein betrieblich genutztes LAN in der Regel als ein Arbeitsmittel anzusehen ist, wird ein privates LAN oftmals für das Hobby und das Vergnügen eingesetzt. Betrieblich und privat sind zunächst zwei völlig verschiedene Nutzungsgebiete, auch wenn für beide möglicherweise typische PCs sowie übliche Programme und das Internet genutzt werden.

Dementsprechend sind auch unterschiedliche Kriterien für die Sicherheit und den Datenschutz anzulegen. Während beispielsweise der Administrator einer Firma keine Videos- und MP3-Dateien auf den Servern duldet und sie beim Auffinden aus den Benutzerverzeichnissen löscht, sind die Firmenangestellten der Meinung, dass dies dem Datenschutz widerspreche, weil Daten in ihren Verzeichnissen als vertraulich einzustufen seien und der Administrator hier deshalb nichts zu suchen habe. Daran ist zu erkennen, dass Sicherheit und Datenschutz im Prinzip zwei kontroverse Themen sind.

Deshalb sollte in einer Firma die Bestimmung und die Verwendung der PCs und des Netzwerkes eindeutig durch eine Dienstanweisung definiert und bei den Anwendern für eine entsprechende Sensibilisierung Sorge getragen werden, denn Sicherheit bedeutet meist auch eine Einschränkung bei der Bedienbarkeit und Funktionalität, was nicht immer sofort akzeptiert wird. Die Dienstanweisung sollte zudem definieren, ob eine private Nutzung des Internet und/oder Emails gestattet sind.



Eine Dienstanweisung sollte eindeutig die Bestimmung und die Verwendung der PCs und des Netzwerkes in einer Firma definieren, denn eine Unterlassung führt häufig zu beiderseitigen Missverständnissen und wirft vermeidbare Sicherheitsprobleme auf.

Oftmals wird stillschweigend davon ausgegangen, dass dies erlaubt sei, wenn es nicht explizit verboten ist, was den Arbeitgeber durchaus in Bedrängnis bringen kann, denn ohne Verbot fungiert er laut TKG (Telekommunikationsgesetz) als Diensteanbieter, der auch eine Vertraulichkeit und Unversehrtheit der Benutzerdaten garantieren muss.

Dies hat genau genommen zur Folge, dass die Daten der Angestellten dann noch nicht einmal nach SPAM oder Viren durchsucht werden dürfen, und dem Administrator ist es unter diesen Umständen tatsächlich nicht erlaubt – sei es manuell oder auch automatisiert per Software –, die Daten aus Sicherheitsgründen zu durchsuchen.

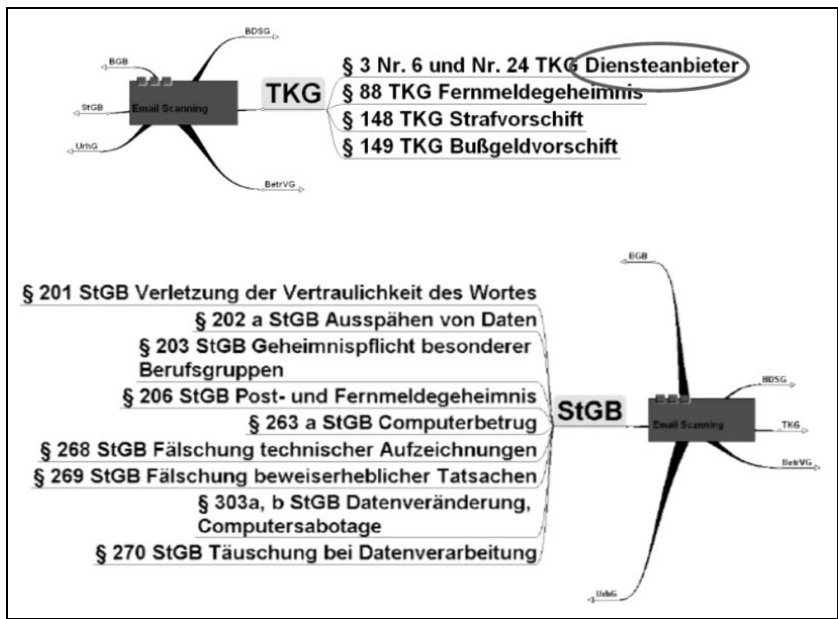


Abbildung 16.2: Zahlreiche Gesetze tangieren direkt oder auch indirekt die IT-Sicherheit und den Datenschutz, wobei hier nur diejenigen gezeigt sind, die die Suche nach Viren tangieren können.

Eine Vielzahl von Gesetzen befassen sich mehr oder weniger direkt mit den Themen IT-Sicherheit und Datenschutz. Deshalb verwundert es nicht, dass es in Schadensfällen recht unterschiedliche Urteile gibt, die meist nach langwierigen Verhandlungen unter Berücksichtigung der individuellen Umstände zustande kommen. Nicht selten wird die Versicherung, die für einen entstandenen Schaden eintreten soll, den Gang durch die Instanzen anstreben.

16.1.1 Viren

Viren sind meist relativ kleine Programme, die in der Lage sind, sich an andere Programme »anzuhängen«, wodurch sie sich reproduzieren und zeitgesteuert Schäden verursachen können.

Viren können über die üblichen Datenträger (Disketten, DVDs, USB-Memory-Sticks) und besonders einfach über das Internet auf den PC gelangen, sobald eine Datei geladen wird. Das Internet ist für Viren deshalb besonders attraktiv, weil es weltumspannend ist und viele potentielle Infektionsopfer bietet. Außerdem ist das Internet weitgehend unkontrolliert, so dass Programme, die Viren enthalten, leicht verbreitet werden können. Die Viren-Autoren bleiben meist anonym, so dass es schwierig ist, sie zur Verantwortung zu ziehen.

Die meisten Viren verraten sich nicht direkt und sofort durch eine Beeinträchtigung der Funktionsweise des Wirtsprogramms oder des Rechners. Häufig schlagen sie erst nach einer bestimmten Zeit (Rechenzeit oder Tageszeit), ab oder an einem bestimmten Datum oder nach erfolgreicher Infektion bestimmter Dateien zu.

Boot-Viren setzen sich in dem Bereich einer Festplatte oder Diskette fest, der beim Starten eines Computers in den Arbeitsspeicher gelesen wird. Wenn der Prozessor das Betriebssystem von der Festplatte startet, lädt er deshalb automatisch den Virus, der daraufhin die Kontrolle über den PC erlangen kann.

Datei-Viren infizieren Programmdateien, wie beispielsweise Spiele oder Betriebssysteme. Wenn der Anwender die befallene Datei startet, infiziert der Virus weitere Dateien und pflanzt sich somit fort. In jeder ausführbaren Datei, wie zum Beispiel *.exe oder *.com, kann sich ein Virus verstecken.



Abbildung 16.3: Der Love Letter-Virus nutzt VBA (Visual Basic).

Auch Textdokumente vom Typ *.doc oder Tabellen vom Typ *.xls können virenverseucht sein. Dies sind dann meist Makroviren, die in Makrosprachen (VBA, Visual Basic for Applications) von Anwendungsprogrammen wie etwa für MS Office verfasst sind und sich in den entsprechenden Dokumenten (.doc, .xls) verbergen können.

Makroviren können sich auch unabhängig vom eingesetzten Betriebssystem fortpflanzen und sind relativ einfach zu programmieren. Sie haben sich in den letzten Jahren durch den zunehmenden Datenaustausch per Email und die Nutzung des Internets schlagartig vermehrt.

Ein Virus ist unabhängig vom jeweiligen Typ meist nach dem folgenden Schema aufgebaut:

- ▶ **Erkennungsteil:** Hiermit stellt der Virus fest, ob die Datei bereits befallen ist, so dass unnötige Mehrfachinfektionen vermieden werden. Der Virus erhöht damit schnell seine Ausbreitung und wird nicht so leicht erkannt.
- ▶ **Infektionsteil:** Dieser Teil wählt ein Programm (das Wirtsprogramm) aus und fügt den Programmcode des Virus ein. Das ausgewählte Programm ist damit infiziert und kann von nun an bei einem Aufruf selbst weitere Programme infizieren.
- ▶ **Funktionsteil:** Im Funktionsteil wird festgelegt, was im System manipuliert werden soll. Um möglichst nicht gleich entdeckt zu werden, sind in vielen Viren so genannte Trigger implementiert. Der Virus wird erst aktiv, wenn ein bestimmtes Ereignis eintritt, zum Beispiel an einem bestimmten Datum oder nach dem x-ten Start eines Programms. Vom einfachen Nichtstun (lediglich Verbreitung) bis zum Löschen der Festplatte ist dabei alles möglich.

Zunehmend stecken Viren auch in Bild- und Sounddateien, was bedeutet, dass noch nicht einmal ein Anhang geöffnet werden muss, sondern die Email nur aufgerufen zu werden braucht, damit der Virus aktiv werden kann.

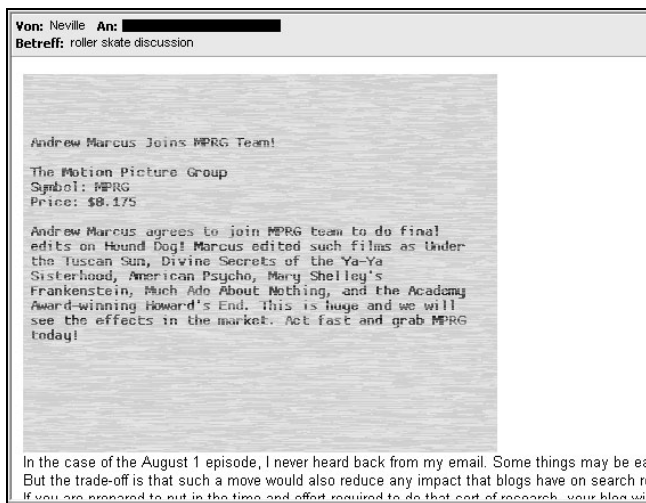


Abbildung 16.4: In dieser Mail steckt der Virus im Hintergrundbild, auf dem der Text steht.

Generell gibt es kein Antiviren-Programm, das alle bekannten Viren detektieren und daraufhin erfolgreich beseitigen kann. Der mitunter zu lesende Tipp, deshalb mehrere unterschiedliche Virens Scanner einzusetzen, damit die Wahrscheinlichkeit steigt, dass möglichst viel erkannt wird, funktioniert deshalb nicht, weil sich die Scanner gegenseitig behindern und bereits die Installation scheitern kann, wenn schon ein anderer Scanner (im Speicher) aktiv ist. Stattdessen sollte die Virens Scanner Software am besten täglich aktualisiert werden, um die ständig neuen Virustypen erkennen zu können. Ein für den Privateinsatz kostenloser Virens Scanner mit guter Aktualisierungsrate ist unter www.freeav.de als *AntiVir Personal Edition* zu finden.

16.1.2 Würmer

Eine Variante von Viren sind die so genannten Würmer. Der erste Wurm bestand aus 99 Zeilen Code und wurde vom Sohn eines NSA-Sicherheitsexperten im Jahre 1988 für UNIX geschrieben. UNIX ist allerdings nicht die bevorzugte Plattform für Schadsoftware, sondern aufgrund der hohen Verbreitung ist dies natürlich Windows.

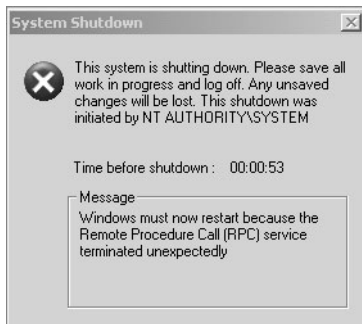


Abbildung 16.5:
Der W32 Blaster-Wurm führt zum Herunterfahren des PC.

Würmer benötigen kein Wirtsprogramm und verbreiten sich meist über Emails. Es sind eigenständige Programme, die für ihre Aktivierung in der Regel eine Aktion des Anwenders erfordern, wie den Aufruf einer an die Email gehängten Datei, und sich anschließend selbst weiterverbreiten. Würmer sind auf die selbstständige Verbreitung in Netzwerken ausgerichtet und können deshalb in kürzester Zeit hunderte von PCs infizieren und diese außer Betrieb setzen.

16.1.3 Trojanische Pferde

Als *Trojanische Pferde* werden Programme mit mehr oder weniger destruktivem Charakter bezeichnet, die neben den spezifizierten Aufgaben auch noch andere Funktionen ausführen, ohne dass die Benutzer dies bemerken.

Meistens werden Trojanische Pferde zum Ausspionieren geheimer Daten eingesetzt. Sie geben sich als scheinbar nützliches Programm aus und werden maskiert in das Computersystem eingeschleust oder auch als Ersatz eines normalen Programms eingeschmuggelt. Damit können beispielsweise Passwörter und andere vertrauliche Daten ausgespäht,

verändert, gelöscht oder bei der nächsten Datenübertragung an den Angreifer verschickt werden. Dieser Datendiebstahl bleibt in der Regel unbemerkt, weil im Gegensatz zum Diebstahl materieller Dinge nichts fehlt.

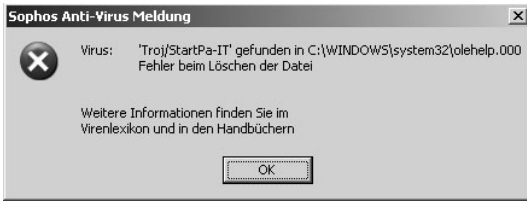


Abbildung 16.6:
Der Trojaner wird zwar als Virus detektiert, er kann von diesem Virenschanner jedoch noch nicht beseitigt werden.

Anders als Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten. Die Verbreitung erfolgt typischerweise durch die folgenden Wege:

- ▶ Durch aktive Inhalte von WWW-Seiten, die aufgrund nicht sicher eingestellter Internet-Browser die Dateien auf die Festplatte kopieren.
- ▶ Durch kostenlose Software, die zum Download im Internet angeboten wird und nicht nur das ausführt, was sie vorgibt.
- ▶ Durch Email-Anhänge, die nach Ausführung ein Trojanisches Pferd auf dem PC installieren.
- ▶ Durch versteckte, aktive Inhalte in HTML-E-mails.

Auf Bestreben der NSA sollen in Windows Vista zahlreiche Mechanismen untergebracht worden sein, die dem Prinzip eines *Trojanischen Pferdes* entsprechen, d.h., mit ihnen können Informationen abgefragt werden, ohne dass es der Anwender bemerkt. Entsprechende Pläne des Bundesinnenministers Schäuble, zwecks Terroristenbekämpfung einen so genannten *Bundestrojaner* auf den PCs einzusetzen, hat es auch bereits gegeben.



Die Sicherheitseinstellungen bei den Web Browsern können in der Praxis nur sehr bedingt für eine erhöhte Sicherheit Sorge tragen. Falls die Ausführung von aktiven Inhalten verboten (ActiveX, VB Script, Java Script, Flash) und die Sicherheitsstufe als hoch konfiguriert wird, lassen sich Seiten im Internet kaum noch vollständig betrachten. Stattdessen ist eine entsprechende Sensibilisierung der Benutzer und eine zentrale Stelle für die Sicherheitsoptionen (Firewall) im Netzwerk weitaus effektiver.

16.1.4 Hoaxes

Hoax ist eine englische Bezeichnung für einen schlechten Scherz. Dieser Begriff hat sich im Internet als Bezeichnung für die zahlreichen falschen Warnungen vor bösartigen Computerprogrammen eingebürgert. Angeblich können Hoaxes Festplatten löschen, Daten ausspionieren oder anderweitig Schaden auf den Rechnern der Betroffenen anrichten.

Nicht nur Neulinge im Netz, sondern auch Administratoren fallen mitunter auf die schlechten Scherze herein, die per Email wie ein Kettenbrief durch das Internet wandern.

Die meisten Hoaxes sind nach dem gleichen Schema verfasst. Sie beginnen mit einem Aufhänger, der Seriosität vermitteln soll. Es folgt die angebliche Aufklärung über die Bedrohung aus dem Netz sowie meist ein Tipp, was dagegen zu tun ist: Etwa *Löschen Sie die Datei xyz*, was nach Befolgung meist nicht mehr als Scherz empfunden wird, weil Windows und/oder bestimmte Software dann nicht mehr funktioniert. Auf jeden Fall enthält der Hoax noch die Bitte, diese Warnung möglichst allen Bekannten zukommen zu lassen.

Echte Virus-Warnungen werden jedoch nie auf diese Weise verschickt. Nur bei den Herstellern von Antivirensoftware oder auch öffentlichen Institutionen – wie dem *Bundesamt für Sicherheit in der Informationstechnik*, www.bsi.bund.de – erhält man seriöse Informationen über drohende Viren.

16.1.5 SPAM

Unter SPAM versteht man unverlangt zugestellte Emails. Die richtige Bezeichnung hierfür ist *Unsolicited Commercial Email (UCE)*, allerdings ist SPAM die gebräuchlichere, die von einem Monty Python-Sketch mit einem Dosenfleisch (Spiced Porc And Ham) abgeleitet worden ist.

Die automatisierte Massensendung von Werbung steht ohne Beziehung zum Empfänger und überflutet nicht selten die Email-Konten, was für einen gewaltigen Internetverkehr sorgt, der auch über Bot-Netze (siehe oben) abgewickelt wird. Nicht nur Werbung, auch Betrügereien werden mit SPAMs versucht, wenn etwa jemand Hilfe benötigt oder auch nicht weiß, wo er mit seinem vielen Geld hin soll.

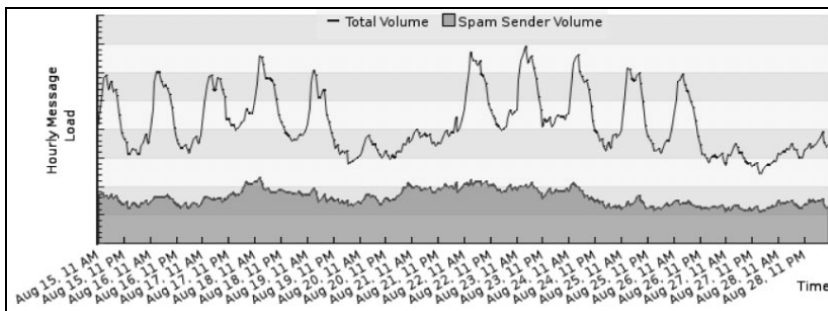


Abbildung 16.7: Der SPAM-Anteil ist bei Emails recht hoch und erzeugt eine unnötige Grundlast im Internet.

Grundsätzlich sollte nie auf eine SPAM-Mail geantwortet werden, weil dies für den Sender zunächst eine Bestätigung dafür ist, dass unter der Email-Adresse tatsächlich jemand zu erreichen ist, der dann gewissermaßen als Dank noch mehr SPAMs erhalten wird. Jedes aktuelle Mailprogramm kennt von Hause aus zumindest einfache, regelbasierte SPAM-Filter. Bei Outlook Express sind diese über EXTRAS -NACHRICHTENREGELN zugänglich.

Typische separate SPAM-Filter-Programme für PCs (z.B. K9 von Robin Keir) sind weit aus intelligenter, weil sie nach statistischen Verfahren arbeiten können und keinesfalls auf manuell zu konfigurierende Regeln angewiesen sind. K9 funktioniert nach einer kurzen Lernphase, in der mit Unterstützung des Anwenders Mails von SPAM zu separieren sind, sehr zuverlässig, ohne dass zuvor jemals eine Filterregel manuell festgelegt werden musste. K9 befindet sich auf der beiliegenden CD. Da es jedoch nur mit POP3 (Post Office Protocol) für den Zugriff und die Verwaltung der Emails, nicht jedoch mit IMAP (Internet Message Access Protocol) arbeiten kann, lässt sich damit nur eine lokale SPAM-Filterung und keine auf dem Mail-Server durchführen.

Um möglichst wenig SPAM zu erhalten, empfiehlt es sich, mit der eigenen Email-Adresse sorgsam umzugehen. Sie sollte also nicht direkt auf einer Internetseite zu finden sein, von wo aus sie unmittelbar in die SPAM-Verteilungsprogramme gelangen kann. Außerdem ist die Verwendung von BBC (Blind Carbon Copy) statt CC im Email-Programm ein probates Mittel, damit Email-Adressen nicht übermäßig im Internet verteilt werden. BBC kann in jedem üblichen Mailprogramm statt CC selektiert werden, womit verhindert wird, dass die Empfängerliste im Header erscheint.

Die Teilnahme an Chats kann geradezu Unmengen an ungewollten Emails zur Folge haben. Beim *Instant Messaging* werden Benutzerdaten in verschiedene Datenbanken eingetragen (MSN, Icq), die von entsprechenden Programmen automatisch durchsucht und dann für die Verteilung von Werbung oder ungewollten Kontaktadressen eingesetzt werden. Die Chatclients selbst sind zwar selbst kein direktes Sicherheitsrisiko, sie werden jedoch in zunehmendem Maße für die Verbreitung von Schädlingen (Trojaner) verwendet.

16.2 Firewalls

Eine Firewall befindet sich an der Schnittstelle zwischen dem eigenen Netzwerk und dem nicht vertrauenswürdigen Internet. Sie wirkt wie eine Sicherheitsschleuse oder wie die Passkontrolle an einem Grenzübergang. Die Aufgabe besteht darin, die Kommunikation zu und von einem Netzwerk anhand von bestimmten Regeln zu erlauben oder zu verbieten.

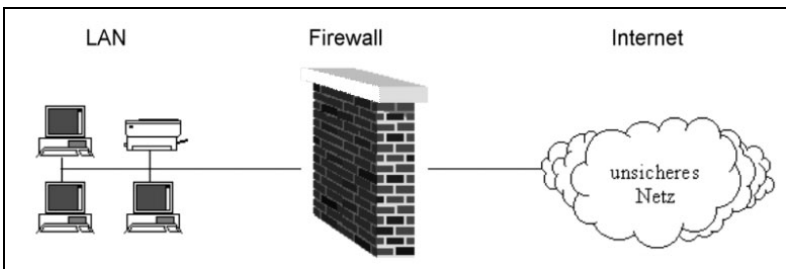


Abbildung 16.8: Eine Netzwerk-Firewall schützt an zentraler Stelle nicht nur einen einzelnen PC, sondern gleich ein komplettes LAN.

Im Buch sind zu den in Windows integrierten Firewalls, die gemeinhin als *Desktop Firewalls* oder auch als *Personal Firewalls* bezeichnet werden, einige Erläuterungen zu finden. Zur gleichen Kategorie gehören die separat erhältlichen Versionen für Windows, beispielsweise die bekannten Programme *McAfee Desktop Firewall*, *Symantec Personal Firewall* oder auch *Zone Alarm* (auf CD).

Personal bedeutet in diesem Zusammenhang, dass die Firewall nach den ganz persönlichen Vorstellungen konfiguriert werden kann und nicht etwa eine separate Firewall gemeint ist, die als ein eigenständiges Gerät ein komplettes LAN vom Internet absichern kann. Der Vorteil einer derartigen *Netzwerk-Firewall* ist wiederum der, dass die Firewall-Regeln nur einmal an zentraler Stelle und nicht bei mehreren PCs konfiguriert werden müssen, was Update und Support wesentlich vereinfacht. Nicht selten arbeitet in diesen Geräten, die letztendlich auch nur PCs sind, ein spezielles »Minimal-Linux« mit Firewall-Software. Die Funktion eines Router kann dabei ebenfalls mit ausgeführt werden.

Eine Netzwerk-Firewall soll den Einbruch in das LAN und das Ausspionieren von Daten verhindern. Die Spionage über das Netzwerk, etwa durch Belauschen des internen Datenverkehrs, ist heutzutage nicht mehr zu unterschätzen, genauso wenig wie die Möglichkeit, PCs in einem LAN, wenn sie schon nicht manipuliert werden können, zumindest durch Attacken aus dem Internet (Denial of Service, Syn Flooding) am normalen Betrieb zu hindern. Maßnahmen hierfür sind:

- ▶ Blockieren von unerwünschtem bzw. unbekanntem Verkehr.
- ▶ Protokollierung des Verkehrs von und zum LAN.
- ▶ Weiterleitung eingehenden Verkehrs an vertrauenswürdige, interne Systeme.
- ▶ Verbergen von kompletten Systemen sowie Informationen wie Systemnamen, Netzwerktopologie, Netzwerk-Gerätetypen und interne Usernamen vor dem Internet.

Grundsätzlich kann man verschiedene Firewall-Konzepte unterscheiden, die auf verschiedenen Levels arbeiten.

Auf der unteren Ebene (OSI-Sicht 3) arbeiten Firewalls mit Paketfiltern, die anhand von IP-Paketen eine Unterscheidung zwischen erlaubten und unerlaubten Verbindungen vornehmen. Hierfür wird eine Liste (State Table) mit Quell- und Zieladresse sowie Quell- und Zielport geführt, die bestimmt, welche Computer im zu schützenden und welche im unsicheren Netzwerk mit welchen Ports und mit welchen Diensten Verbindungen aufnehmen dürfen. Die jeweiligen Antwortpakete (aus dem Internet) werden üblicherweise zugelassen, was als *Stateful Filter* bezeichnet wird.

Die Filterregeln sind an die Netzwerkschnittstellen gebunden und werden vom Paketfilter in der Reihenfolge abgearbeitet, in der sie angegeben sind.

Die Paketfilterung ist eine kostengünstige Technologie, die bei fast allen Router-Produkten standardmäßig implementiert ist. Der Konfigurationsaufwand hält sich in Grenzen, und wenn neue Dienste oder Protokolle transportiert werden müssen, lassen sich neue Regeln relativ leicht einführen.



Die grundlegende Regel für die Paketfilterung ist die Dioden-Regel: *Der Verkehr aus dem LAN ins Internet wird erlaubt, nicht jedoch in umgekehrter Richtung.* Als allgemeine Filterregel gilt schlechthin: *Alles, was nicht ausdrücklich erlaubt wurde, ist verboten.*

Auf der OSI-Schicht 4 (TCP, UDP) arbeitet eine flexiblere Variante, denn eine starre Tabelle ist für einige Protokolle, wenn etwa variable Portnummern verwendet werden, ungeeignet. Eine *Stateful Inspection Firewall* passt die Firewall-Regeln dynamisch an, so dass neue, notwendige Ports für eine bestimmte Anwendung berücksichtigt werden können. Eine derartige zustandsgesteuerte Firewall enthält auch die Tabellen für die statischen Paketfilter.

Damit kann im IP-Header die Filterung nach IP-Adressen erfolgen, im TCP/UDP-Header nach Portnummern, im jeweiligen Dienst nach Protokollnummern (Datagrammtyp), und die Richtungsfeststellung erfolgt durch die Auswertung des Syn-/Ack-Flags (vgl. Kapitel 7.1).

Als Nachteile ist zu werten, dass die Regeln für den Durchschnittsbenutzer oft recht verwirrend wirken und auch sehr umfangreich und schwer nachvollziehbar sein können, schließlich sind Regeln für beide Richtungen festzulegen. Außerdem können die Inhalte der Datagramme nicht kontrolliert werden, und es gibt auf dieser Ebene keine Authentifizierung der Benutzer.

Das zweite grundlegende Firewall-Konzept ist deshalb die Kontrolle der Kommunikationsbeziehungen auf der Anwendungs- und nicht auf der Paketebene, was auch unter *Application Level Firewall* firmiert.

Typischerweise wird dabei für jeden Dienst (Telnet, FTP, WWW, Email) ein *Security Proxy* eingefügt, was einem Zwischenspeicher entspricht, der den direkten Zugriff auf den jeweiligen Dienst unterbindet und dadurch eine Analyse der Inhalte ermöglicht. Diese können je nach Firewall-Konfiguration erlaubt oder abgeblockt werden, was auch benutzerabhängig stattfinden kann, weil eine Authentifizierung der Benutzer möglich ist. Idealerweise kann die Firewall in eine Active Directory-Struktur integriert werden, was eine zentrale Authentifizierung gestattet.



Network Firewalls kombinieren das Prinzip von Packet Firewall, Stateful Inspection Firewall und Application Firewall.

Eine ausgewiesene Netzwerk-Firewall unterstützt nicht nur zwei Netzwerkschnittstellen für die Verbindung zwischen LAN und Internet, sondern meist noch mindestens eine weitere, die für den Aufbau einer so genannten *Demilitarized Zone* (DMZ) bestimmt ist.

Hiermit wird die Firewall funktionell quasi in zwei Teile gespalten und in der Mitte kann diese »entmilitarisierte« Zone angeschlossen werden, die typischerweise für einen WWW- und einen Mail-Server zum Einsatz kommt. Diese beiden Servertypen sind naturgemäß mit dem Internet verbunden, und die hierfür bestimmten Pakete erfahren bei der Firewall-Lösung (Port A) zunächst eine entsprechende Vorfilterung in der DMZ (Port B), bevor sie mithilfe der Clients die Berechtigung erhalten, ins LAN (Port C) zu gelangen.

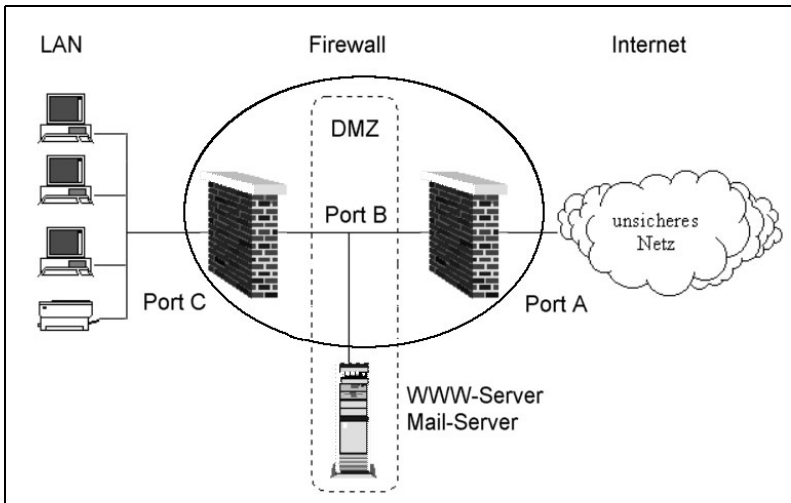


Abbildung 16.9: Netzwerk-Firewalls erlauben zumeist auch die Realisierung einer DMZ.

16.2.1 Routing Firewall

Das Prinzip einer gebräuchlichen Firewall beruht auf dem *Routing*, d.h. dem Übergang von einem Netz zu einem anderen. Hierfür verfügt eine Netzwerk-Firewall oder auch ein hierfür abgestellter Server mindestens über zwei Netzwerkkarten, die sich mit ihren IP-Adressen in zwei unterschiedlichen Netzen befinden.

Als Beispiel wird hierfür zunächst ein Linux-PC mit zwei Netzwerkkarten und der *Personal Firewall* von SuSE verwendet, die das Masquerading ohne aufwändigere Konfigurationsarbeiten ermöglicht. Auch wenn es *Personal Firewall* heißt, kann der Linux-PC mit der beschriebenen Konfiguration als eigenständige Firewall zwischen zwei Netzen fungieren. Für die Verbindung zweier Netze (Routing) muss der Eintrag `IP_FORWARD="yes"` in der Datei `/etc/rc.config` gesetzt werden.

In der Netzwerkumgebung eines PC am internen Netz tauchen lediglich die LAN-Clients auf, und es gibt zunächst keinen Zugriff auf das Internet. Damit der PC die Zugriffsmöglichkeit auf dieses externe Netz erhält, muss zunächst seine Adresse maskiert (Masquerading) werden.

Die Festlegungen für die Personal Firewall finden sich unter `/etc/rc.config.d/` in der Datei `security.rc.config`. Damit das Masquerading zwischen internem und externem Netzwerk über diese Firewall ausgeführt werden kann, ist lediglich der Eintrag `REJECT_ALL_INCOMING_CONNECTIONS="masq"` zu setzen. Wird statt »masq« hier »no« angegeben, ist die Personal Firewall und damit das Masquerading außer Betrieb.

Eine Firewall-Funktion ist bis hierhin nicht gegeben, es findet lediglich das Masquerading auf Grund des `masq`-Eintrages statt. Damit explizit alle eingehenden Verbindungen zu `Eth0` (aus dem Internet) unterbunden werden, ist `REJECT_ALL_INCOMING_CONNECTIONS="eth0 masq"` zu setzen. Damit funktioniert auch kein Ping mehr auf die externe IP-Adresse, und die Personal Firewall erfüllt nunmehr ihren Dienst.

Einen größeren Funktionsumfang als die Personal Firewall bietet die SuSEfirewall, bei der sich zahlreiche Filteroptionen einstellen lassen. Die Konfigurierung kann über YaST erfolgen oder auch durch die direkte Anpassung der dazugehörigen Konfigurationsdatei unter `/etc/rc.config.d/firewall.rc.config`

Die SuSEfirewall stellt im Prinzip nur ein Skript dar, welches die IPCHAINS (Paketfiltereinstellungen) entsprechend manipuliert. Ab dem Kernel 2.4 sollen statt der IPCHAINS die IPTABLES eingesetzt werden, die beispielsweise ab der SuSEfirewall2 standardmäßig zum Einsatz kommen. IPCHAINS mit Kernel 2.4 erlaubt beispielsweise kein FTP.

Anzeige der IPCHAINS/IPTABLES-Einstellungen:

```
ipchains -L
iptables -L
```

Der automatische Start der SuSEfirewall erfolgt durch den Eintrag `START_FW="yes"` in der Datei `/etc/rc.config`. Der Eintrag ist am Ende der Datei lokalisiert.

Manuelle Aufrufe mit:

```
SuSEfirewall -h (Optionen anzeigen)
SuSEfirewall (starten)
SuSEfirewall stop (stoppen)
SuSEfirewall check (Anzeige der offenen Ports)
```

Bei dem *SuSEfirewall Check* tauchen möglicherweise Fehlermeldungen auf, die aber ignoriert werden können, wenn die grundsätzliche Funktion der Firewall gegeben ist. Hierfür sollte die Ping-Option in `/etc/rc.config.d/firewall.rc.config` (Option 19) für Eth0 (externes Netz) aktiviert und wieder deaktiviert werden.

Ein Ping vom externen Netz führt bei aktivierter Firewall zu keiner Antwort eines PC im LAN. Ein Ping aus dem internen Netz (da Masquerading) auf diese Adresse sollte hingegen stets funktionieren.

Inhalt der Datei `firewall.rc.config`:

```
# Copyright (c) 1999-2001 SuSE GmbH Nuernberg, Germany. All rights reserved.
# Angepasst: K.D. 23.05.04
# /etc/rc.config.d/firewall.rc.config
# for use with /sbin/SuSEfirewall version 5.0
#
# Configuration HELP:
# If you have got problems configuring this file, take a look at
# /usr/share/doc/packages/SuSEfirewall/EXAMPLES for an example.
#
# 1.)
# Should the Firewall be started?
# This setting is done in /etc/rc.config (START_FW="yes")
#
```

Firewalls

```
# 2.)
# Which is the interface that points to the internet?
FW_DEV_WORLD="eth0"
#
# 3.)
# Which is the interface that points to the internal network?
FW_DEV_INT="eth1"
#
# 4.)
# Which is the interface that points to the dmz network?
FW_DEV_DMZ=""
#
# 5.)
# Should routing between the internet, dmz and internal network be activated?
FW_ROUTE="yes"
#
# 6.)
# Do you want to masquerade internal networks to the outside?
FW_MASQUERADE="yes"
#
# Which internal computers/networks are allowed to access the internet
# directly (not via proxys on the firewall)?
# Only these networks will be allowed access and will be masqueraded!
#
FW_MASQ_NETS="192.168.0.0/24"
#
# If you want (and you should) you may also set the FW_MASQ_DEV option, to
# specify the outgoing interface to masquerade on. (You would normally use
# the external interface(s), the FW_DEV_WORLD device(s), e.g. "ipp0")
FW_MASQ_DEV="$FW_DEV_WORLD"
#
# 7.)
# Do you want to protect the firewall from the internal network?
# REQUIRES: FW_DEV_INT
#
# If you set this to "yes", internal machines may only access services on
# the machine you explicitly allow. They will be also affected from the
# FW_AUTOPROTECT_GLOBAL_SERVICES option.
# If you set this to "no", any user can connect (and attack) any service on
# the firewall.
#
FW_PROTECT_FROM_INTERNAL="no"
#
```

```

# 8.)
# Do you want to autoprotect all global running services?
#
# If set to "yes", all network access to services TCP and UDP on this machine
# which are not bound to a special IP address will be prevented (except to
# those which you explicitly allow, see below: FW_*_SERVICES_*)
# Example: "0.0.0.0:23" would be protected, but "10.0.0.1:53" not.
#
FW_AUTOPROTECT_GLOBAL_SERVICES="yes"
#
# 9.)
# Which services ON THE FIREWALL should be accessible from either the internet
# (or other untrusted networks), the dmz or internal (trusted networks)?
# (see no.13 & 14 if you want to route traffic through the firewall)
#
# Enter all ports or known portnames below, seperated by a space.
# TCP services (e.g. SMTP, WWW) must be set in FW_SERVICES_*_TCP, and
# UDP services (e.g. syslog) must be set in FW_SERVICES_*_UDP.
# e.g. if a webserver on the firewall should be accessible from the internet:
# FW_SERVICES_EXTERNAL_TCP="www"
# e.g. if the firewall should receive syslog messages from the dmz:
# FW_SERVICES_DMZ_UDP="syslog"
# For IP protocols (like GRE for PPTP, or OSPF for routing) you need to set
# FW_SERVICES_*_IP with the protocol name or number (see /etc/protocols)
#
# Choice: leave empty or any number of ports, known portnames (from
# /etc/services) and port ranges seperated by a space. Port ranges are
# written like this, from 1 to 10: "1:10"
# e.g. "", "smtp", "123 514", "3200:3299", "ftp 22 telnet 512:514"
# For FW_SERVICES_*_IP enter the protocol name (like "igmp") or number ("2")
#
# Services, visible to the external net (normally internet), TCP
# Common: smtp domain
FW_SERVICES_EXTERNAL_TCP=""
# Services, visible to the external net (normally internet), UDP
# Common: domain
FW_SERVICES_EXTERNAL_UDP=""
# Externally visible services, other IP protocols
# For VPN/Routing which END at the firewall!!
FW_SERVICES_EXTERNAL_IP=""
#
# Services visible to the DMZ, TCP
# Common: smtp domain
FW_SERVICES_DMZ_TCP=""

```

Firewalls

```
# Services visible to the DMZ, UDP
# Common: domain syslog
FW_SERVICES_DMZ_UDP=""
# Services visible to the DMZ, other IP protocols
# For VPN/Routing which END at the firewall!!
FW_SERVICES_DMZ_IP=""
#
# Services, visible to the internal net, TCP
# Common: ssh smtp domain
FW_SERVICES_INTERNAL_TCP="1:65535"
# Services, visible to the internal net, UDP
# Common: domain syslog
FW_SERVICES_INTERNAL_UDP=""
# For VPN/Routing which END at the firewall!!
FW_SERVICES_INTERNAL_IP=""
#
# 10.)
# Which services should be accessible from trusted hosts/nets on the internet?
#
# Define trusted networks on the internet, and the TCP and/or UDP services
# they are allowed to use.
#
# Choice: leave FW_TRUSTED_NETS empty or any number of computers and/or
# networks, seperated by a space. e.g. "172.20.1.1", "172.20.0.0/16"
#
FW_TRUSTED_NETS="134.28.0.0/16"
#
# leave FW_SERVICES_TRUSTED_* empty or any number of ports, known portnames
# (from /etc/services) and port ranges seperated by a space.
# e.g. "25", "ssh", "1:65535", "1 3:5"
# ..._IP needs IP protocol names or numbers and does not support ranges!
#
# Services, available to trusted hosts/nets, TCP
# Common: ssh
FW_SERVICES_TRUSTED_TCP=""
# Services, available to trusted hosts/nets, UDP
# Common: syslog time ntp
FW_SERVICES_TRUSTED_UDP=""
# Services, available to trusted hosts/nets, other IP protos
# For VPN/Routing which END at the firewall!!
FW_SERVICES_TRUSTED_IP=""
# Some people want to allow some trusted machines access to some services
# and different services to others. OK, here is your hardcore config option:
# "trusted_net,protocol,port" e.g. "10.0.1.0/24,tcp,80 10.0.1.6,tcp,21"
FW_SERVICES_TRUSTED_ACL=""
#
```

```

# 11.)
# How is access allowed to high (unprivileged [above 1023]) ports?
#
# You may either allow everyone from anyport access to your highports ("yes"),
# disallow anyone ("no"), anyone who comes from a defined port (portnumber or
# known portname) [note that this is easy to circumvent!], or just your
# defined nameservers ("DNS").
# Note that if you want to use normal (active) ftp, you have to set the TCP
# option to ftp-data. If you use passive ftp, you don't need that.
# Note that you can't use rpc requests (e.g. rpcinfo, showmount) as root
# from a firewall using this script (well, you can if you include range
# 600:1023 in FW_SERVICES_EXTERNAL_UDP ...).
#
# Choice: "yes", "no", "DNS", portnumber or known portname, defaults to "no"
#
# Incoming connections on ports >= 1024, TCP
# Common: "ftp-data" (sadly!)
FW_ALLOW_INCOMING_HIGHPORTS_TCP="no"
# Incoming connections on ports >= 1024, UDP
# Common: "DNS" or "domain ntp"
FW_ALLOW_INCOMING_HIGHPORTS_UDP="no"
#
# 12.)
# Are you running some of the services below?
# They need special attention - otherwise they won't work!
#
# Set services you are running to "yes", all others to "no", defaults to "no"
#
# if yes, FW_SERVICES_*_TCP needs to have port 53
# (or "domain") set to allow incoming queries.
# also FW_ALLOW_INCOMING_HIGHPORTS_UDP needs to be "yes"
FW_SERVICE_DNS="no"
# if you use dhclient to get an ip address
# you have to set this to "yes" !
FW_SERVICE_DHCLIENT="no"
# set to "yes" if this server is a DHCP server
FW_SERVICE_DHCPD="no"
# set to "yes" if this server uses samba as client
# or server. As a server, you still have to set
# FW_SERVICES_{WORLD,DMZ,INT}_TCP="139"
# Everyone may send you udp 137/138 packets if set
# to yes! (samba on the firewall is not a good idea!)
FW_SERVICE_SAMBA="yes"
#

```

Firewalls

```
# 13.)
# Which services accessed from the internet should be allowed to the
# dmz (or internal network - if it is not masqueraded)?
# REQUIRES: FW_ROUTE
#
# With this option you may allow access to e.g. your mailserver. The
# machines must have valid, non-private, IP addresses which were assigned to
# you by your ISP. This opens a direct link to your network, so only use
# this option for access to your dmz!!!!
#
# Choice: leave empty (good choice!) or use the following explained syntax
# of forwarding rules, seperated each by a space.
# A forwarding rule consists of 1) source IP/net, 2) destination IP (dmz/intern)
# and 3) destination port (or IP protocol), seperated by a comma (","), e.g.
# "4.0.0.0/8,1.1.1.1,22" [means: net 4.0.0.0 with netmask 255.0.0.0 is
# allowed to connect to the single server 1.1.1.1 on port 22 (which is SSH)]
# "4.4.4.4/12,20.20.20.20,22 12.12.12.12/12,20.20.20.20,22"
# For FW_FORWARD_IP it is "4.0.0.0/8,1.1.1.1,igmp" or "4.0.0.0/8,1.1.1.1"
#
# Forward TCP connections
# Beware to use this!
FW_FORWARD_TCP=""
# Forward UDP connections
# Beware to use this!
FW_FORWARD_UDP=""
# Forward other IP protocol connections (for VPN setups)
# Beware to use this!
FW_FORWARD_IP=""
#
# 14.)
# Which services accessed from the internet should be allowed to masqueraded
# servers (on the internal network or dmz)?
# REQUIRES: FW_ROUTE, FW_MASQUERADE
#
# With this option you may allow access to e.g. your mailserver. The
# machines must be in a masqueraded segment and may not have public IP addresses!
# Hint: if FW_DEV_MASQ is set to the external interface you have to set
# FW_FORWARD_* from internal to DMZ for the service as well!
#
# Please note that this should *not* be used for security reasons! You are
# opening a hole to your precious internal network. If e.g. the webserver there
# is compromised - your full internal network is compromised!!
#
# Choice: leave empty (good choice!) or use the following explained syntax
# of forward masquerade rules, seperated each by a space.
# A forward masquerade rule consists of 1) source IP/net, 2) destination IP
# (dmz/intern) and 3) destination port, seperated by a comma (","), e.g.
```

```

# "4.0.0.0/8,1.1.1.1,22",
# "4.4.4.4/12,20.20.20.20,22 12.12.12.12/12,20.20.20.20,22"
#
# Forward TCP connections to masqueraded host
# Beware to use this!
FW_FORWARD_MASQ_TCP=""
# Forward UDP connections to masqueraded host
# Beware to use this!
FW_FORWARD_MASQ_UDP=""
# it is not possible to masquerade other IP protocols, hence no _IP variable
#
# 15.)
# Which accesses to services should be redirected to a localport on the
# firewall machine?
#
# This can be used to force all internal users to surf via your squid proxy,
# or transparently redirect incoming webtraffic to a secure webserver.
#
# Choice: leave empty or use the following explained syntax of redirecting
# rules, seperated by a space.
# A redirecting rule consists of 1) source IP/net, 2) destination IP/net,
# 3) original destination port and 4) local port to redirect the traffic to,
# seperated by a colon. e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
# Redirect TCP connections
FW_REDIRECT_TCP=""
# Redirect UDP connections
FW_REDIRECT_UDP=""
#
# 16.)
# Which logging level should be enforced?
# Was soll in die Log-Datei geschrieben werden?
# Die Log-Datei ist /var/log/messages
# You can define to log packets which were accepted or denied.
# You can also the set log level, the critical stuff or everything.
# Note that logging *_ALL is only for debugging purpose ...
#
# Choice: "yes" or "no", FW_LOG_*_CRIT defaults to "yes",
# FW_LOG_*_ALL defaults to "no"
#
# Log critical denied network packets
FW_LOG_DENY_CRIT="yes"
# Log all denied packets
FW_LOG_DENY_ALL="no"
# Log critical accepted packets
FW_LOG_ACCEPT_CRIT="yes"

```

Firewalls

```
# Log all accepted packets
FW_LOG_ACCEPT_ALL="no"
#
# 17.)
# Do you want to enable additional kernel TCP/IP security features?
# If set to yes, some obscure kernel options are set.
# (icmp_ignore_bogus_error_responses, icmp_echoreply_rate,
# icmp_destunreach_rate, icmp_paramprob_rate, icmp_timeexceed_rate,
# ip_local_port_range, log_martians, mc_forwarding, mc_forwarding,
# rp_filter, routing flush)
# Tip: Set this to "no" until you have verified that you have got a
# configuration which works for you. Then set this to "yes" and keep it
# if everything still works. (It should!) ;- )
#
# If you are using VPNs (e.g. FreeSWAN) or are combining several ISDN lines
# or similar to one, you have to set this to "no" !
#
# Choice: "yes" or "no", defaults to "yes"
#
FW_KERNEL_SECURITY="no"
#
# 18.)
# Keep the routing set on, if the firewall rules are unloaded?
# REQUIRES: FW_ROUTE
#
# If you are using diald, or automatic dialing via ISDN, if packets need
# to be sent to the internet, you need to turn this on. The script will then
# not turn off routing and masquerading when stopped.
# You might also need this if you have got a DMZ.
# Please note that this is insecure! If you unload the rules, but are still
# connected, you might your internal network open to attacks!
# The better solution is to remove "/sbin/SuSEfirewall stop" or
# "/sbin/init.d/firewall stop" from the ip-down script!
#
# Choices "yes" or "no", defaults to "no"
#
FW_STOP_KEEP_ROUTING_STATE="no"
#
# 19.)
# Allow (or don't) ICMP echo pings on either the firewall or the dmz from
# the internet?
# REQUIRES: FW_ROUTE for FW_ALLOW_PING_DMZ
#
# Choice: "yes" or "no", defaults to "no"
#
```

```

# Allow ping on firewall
FW_ALLOW_PING_FW="no"
# Allow ping on DMZ targets
FW_ALLOW_PING_DMZ="no"
###
# END of firewall.rc.config
###
#
#
#-----#
#
#
# EXPERT OPTIONS - all others please don't change these! #
#
#-----#
#
#
# 20.)
# Allow (or don't) ICMP time-to-live-exceeded to be send from your firewall.
# This is used for traceroutes to your firewall (or traceroute like tools).
#
# Please note that the unix traceroute only works if you say "yes" to
# FW_ALLOW_INCOMING_HIGHPORTS_UDP, and windows traceroutes only if you say
# "yes" to FW_ALLOW_PING_FW
#
# Choice: "yes" or "no", defaults to "no"
#
FW_ALLOW_FW_TRACEROUTE="no"
#
# 21.)
# Allow ICMP sourcequench from your ISP?
#
# If set to yes, the firewall will notice when connection is choking, however
# this opens yourself to a denial of service attack. Choose your poison.
#
# Choice: "yes" or "no", defaults to "yes"
#
FW_ALLOW_FW_SOURCEQUENCH="no"
#
# 22.)
# Which masquerading modules should be loaded?
# REQUIRES: FW_ROUTE, FW_MASQUERADE
#
# (omit the path or "ip_masq_" prefix as well as the ".o" suffix!)
#

```

```
# FW_MASQ_MODULES="autofw cuseeme ftp irc mfw portfw quake raudio user vdolive"
#
# 23.)
# Do you want to load customary rules from a file?
#
# This is really an expert option. NO HELP WILL BE GIVEN FOR THIS!
# READ THE EXAMPLE CUSTOMARY FILE AT /etc/rc.config.d/firewall-custom.rc.config
#
#FW_CUSTOMRULES="/etc/rc.config.d/firewall-custom.rc.config"
```

Die neuere SuSEfirewall2 arbeitet standardmäßig mit IPTABLES, was flexiblere Einstellungen als IPCHAINS erlaubt. Sie ersetzt komplett die vorherige SuSEfirewall, d.h., die Konfigurationsdatei und auch die Bootmeldungen beziehen sich nunmehr auf die SuSEfirewall2, und die vorherigen Einstellungen sind überschrieben, wenn vor der Firewall-Installation keine Sicherheitskopie angelegt wurde. Der Aufbau der *firewall.rc.config* ist jedoch im Wesentlichen mit der vorherigen Konfigurationsdatei identisch.

In der Datei */etc/rc.config* ist dementsprechend der Eintrag `START_FW2=` auf "yes" zu setzen, damit die Firewall beim Start automatisch aktiviert wird. Für das Routen ist hier `IP_FORWARD=` mit "yes" zu versehen. Die Optionen und der Status der SuSEfirewall2 (start, stop, test) lassen sich mit *SuSEfirewall2 -h* anzeigen.

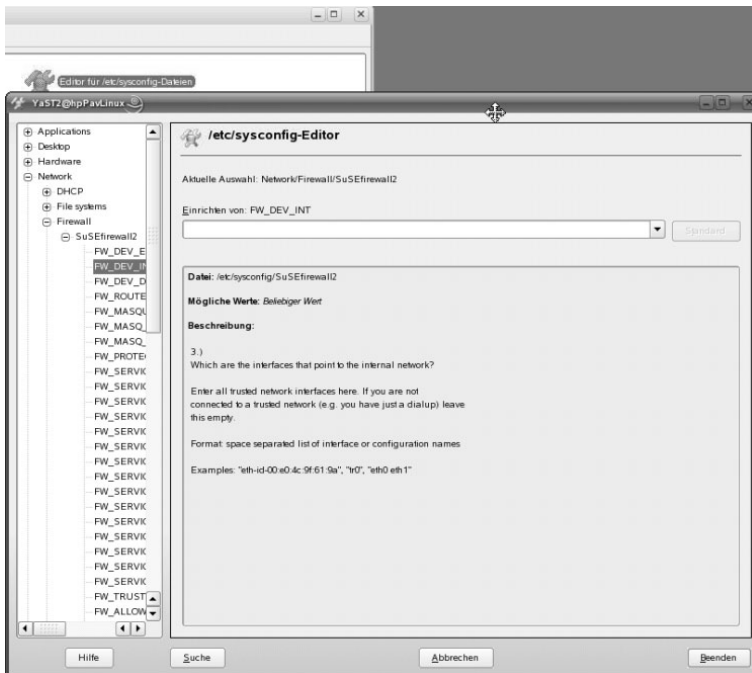


Abbildung 16.10: Die Firewall kann mit dem Editor konfiguriert werden.

Wie in Kapitel 14.2 erwähnt, sind die Konfigurationsdateien bei neueren SuSE-Linux-Versionen unter *etc/sysconfig* zu finden, was auch für die Firewall gilt. YaST stellt einen eigenen Editor (Abbildung 16.10) unter SYSTEM zur Verfügung, damit sich die Konfigurationsdateien bequemer editieren lassen. Außerdem lässt sich die Firewall über YAST – SICHERHEIT UND BENUTZER auch menügeführt aktivieren und konfigurieren, wobei jedoch nicht alle Optionen wie bei der manuellen Einrichtung per Editor in der Datei *SuSEfirewall2* zur Verfügung stehen.

16.2.2 Bridge Firewall

Die übliche Firewall, die auf dem Routing beruht, hat den Nachteil, dass zwei Teilnetze benötigt werden, denn ein Router arbeitet auf der OSI-Schicht 3, d.h., die Wegfindung findet letztendlich auf Grund der IP-Adressen anhand einer Routing-Tabelle statt.

Wenn nur ein einziges Netz mit im Internet gültigen IP-Adressen zur Verfügung steht, ist hier kein Routing und damit auch keine Netzwerk-Firewall realisierbar. Dann müsste ein Teilnetz, etwa mit privaten Adressen, angelegt werden, um zwischen diesen beiden Netzen (Internet, privat) routen zu können, wie es im vorherigen Kapitel erläutert ist. Dies hat jedoch eine Veränderung eines bereits bestehenden Netzes zur Folge, und beim Ausfall des Router ist eine Kommunikation zwischen den beiden Netzen nicht mehr möglich.

Wenn weder die Netzwerkadressen im LAN noch die Netzwerk-Topologie durch die Einführung einer Netzwerk-Firewall verändert werden sollen, kann die Lösung eine Bridging-Firewall sein. Eine Bridge überträgt die Daten über die OSI-Schicht 2, und wie bei einem Switch findet die Kommunikation dabei auf MAC- und nicht auf TCP/IP-Ebene statt. Die Bridge stellt sich im Netzwerk daher als transparent dar und »lernt« durch die Auswertung der MAC-Adressen die Wege zu/von den einzelnen PCs.

Falls die Bridge-Firewall ausfallen sollte, ist lediglich das Netzkabel umzustecken, also die Firewall zu umgehen, wobei keine Adressen zu ändern sind, weil kurzzeitig ohne Firewall gearbeitet wird.

Bei der Verwendung eines üblichen PC als Bridge hat man alle Freiheiten für den Einsatz der jeweiligen Netzwerkadapter (TP, LWL, 100 MBit, Gigabit) und für die festzulegenden Firewall-Regeln, die einfach per Skript anzupassen sind. Diese Kombination ist deshalb gut für den Selbstbau geeignet.

Linux bietet ab dem Kernel 2.6 die benötigte Bridge-Unterstützung, so dass möglicherweise noch eine Aktualisierung notwendig ist, die man am besten aus dem Internet von <http://www.kernel.org> bezieht. Des Weiteren ist die Bridge-Erweiterung noch mit im Kernel unterzubringen. Die notwendigen Bridge-Utilities sind unter <http://bridge.sourceforge.net> zu finden. Bei der Konfigurierung des neuen Kernel sind die *Network Options* und der Punkt *Network Packet Filtering* von Bedeutung, wo man am besten alle Optionen selektiert (* = build in).

Nach dem Start mit dem neuen Kernel sind die Netzwerkkarten zunächst wie üblich von innen und außen über die jeweiligen IP-Adressen per Ping erreichbar. Zuvor sind auf jeden Fall noch das Routing und die möglicherweise vorhandene Firewall zu deaktivieren.

Um die Bridge-Funktion zu starten, ist ein kleines Skript (siehe folgendes Kapitel) empfehlenswert. Die Firewall-Regeln bringt man hier am besten auch gleich mit unter. Nach dem Aufruf des Skripts, bei dem für den Test zunächst keine Firewall-Regeln aktiviert sind, lassen sich bei dem Bridge-PC keine IP-Adressen mehr per Ping ansprechen und die Bridge arbeitet transparent, quasi von einer Netzwerkkarte durch den Kernel hindurch zur anderen Netzwerkkarte. Damit ist die Bridge im Netzwerk nicht erkennbar und belegt auch keine IP-Adressen.

Demnach ist unmittelbar nach dem Anschluss der beiden Netzwerkkarten (eth0:extern, eth1: intern) und dem Aufruf des Bridge-Skriptes eine Kommunikation von den PCs im internen Netz nach außen hin und in umgekehrter Richtung möglich. Der Aufbau einer Internetseite dauert dabei zunächst etwas länger, weil die Bridge den Weg durch das Netz erst noch »lernen« muss. Diese Verzögerung wird bei einem späteren, erneuten Aufruf jedoch nicht mehr weiter auffallen.

Die grundsätzliche Funktion der Bridge ist damit gegeben, und sie kann einfach zwischen den Internet-Anschluss und das interne Netz geschaltet werden, was keinerlei Auswirkungen auf die bereits vergebenen IP-Adressen und die vorhandene Netzwerktopologie hat, weil sie eben völlig transparent wirkt.

Danach sind die Firewall-Regeln festzulegen, was einige Zeit zum Ausprobieren in Anspruch nimmt, damit der gewünschte und der unerwünschte Datenverkehr optimal geregelt werden. Dabei wird ausschließlich mit IPTABLES und FORWARD gearbeitet. Wie die Daten die Regeln INPUT, OUTPUT und eben FORWARD durchlaufen, unterscheidet sich dabei von den älteren Regeln, die mit IPCHAINS gebildet werden.

Firewall-Skript

Das Skript wird mit *mstbridge.sh* aufgerufen, woraufhin eine entsprechende Meldung (Bridge wird gestartet) erscheint. Beim Ausprobieren der Bridge mit der Firewall-Funktion haben sich die folgenden Kommandos als hilfreich erwiesen:

- ▶ `ifconfig mstbridge down`, Deaktivieren der Bridge/Firewall
- ▶ `iptables -L`, Anzeige der aktiven iptables-Regeln
- ▶ `iptables -F`, Löschen aller iptables-Regeln
- ▶ `mstbridge.sh`, Erneutes Starten der Bridge/Firewall

Beim erneuten Starten der Bridge/Firewall können die Fehlermeldungen (already exists ...) ignoriert werden können. Die Bridge wird tatsächlich mit den zuvor getätigten Änderungen neu gestartet, woraufhin die Befehle in Kraft treten. Falsche Angaben (Tippfehler usw.) im Skript werden hingegen durch eine Error-Meldung mit dem Hinweis, die Hilfe zu IPTABLES aufzurufen, ausgewiesen.

Auch nach der Deaktivierung der Bridge (`ifconfig bridge down`) führt ein Ping nicht zu einer Antwort, dies funktioniert nur, bevor das Skript das erste Mal aufgerufen worden ist.

Beim Ausprobieren der Firewall können die Windows-PCs für (scheinbare) Probleme sorgen, wenn etwa keine Seite im Internet aufgerufen werden kann. Der Explorer wie auch die Netzwerkumgebung merken sich vorherige, und falls sich an der Firewall-Einstellung etwas geändert hat, wird zunächst einer der älteren Wege mit den bekannten Optionen eingeschlagen, obwohl er nicht korrekt durchlaufen werden kann. Nach einem

kompletten Durchlauf des Explorers ins Leere (Meldung: Seite kann nicht angezeigt werden) ist dieser dann zu beenden und neu zu starten, woraufhin die Wegfindung wieder funktioniert.

Bei der Erstellung der Regeln für die Firewall mit IPTABLES ist zu beachten, dass die Regeln der Reihe nach – quasi von oben nach unten – durchlaufen werden. Daher macht es beispielsweise keinen Sinn, den Zugriff auf eine bestimmte IP-Adresse oder Ports zu verbieten, wenn zuvor der Verkehr von innen nach außen (und als ESTABLISHED in Gegenrichtung) erlaubt worden wäre. Die verbotene IP-Adresse würde dann als eine etablierte Verbindung angesehen werden und das Verbot nie greifen; es muss deshalb vor den allgemeinen Freigaberegeln stehen.

Die beste Lösung ist es, nur die für bestimmte Anwendungen (http, FTP, DNS) reservierten Ports zu erlauben. Diese Ports sind zwar definiert (80, 21, 53), allerdings werden die ausgehenden Pakete (von den Windows-Clients) nicht auf ihnen, sondern auf wechselnden, höheren (1000-13xx) Ports gesendet. Für die Antwortpakete werden jedoch stets die definierten Ports verwendet. Deshalb wird die Firewall – das Skript – so ausgelegt, dass eine Verbindung stets nur aus dem internen Netz initiiert werden kann und die Antworten aus dem Internet jeweils zu dieser aufgebauten, etablierten Verbindung gehören müssen. Demnach ist es nicht möglich, eine (neue) Verbindung von außen aufzubauen. Vor dieser Festlegung wird der Zugriff auf Ports oberhalb 1400 allerdings explizit verboten, denn es konnte festgestellt werden, dass keine übliche Verbindung auf den Ports oberhalb 1400 notwendig ist.

Falls eine Internet-Verbindung beispielsweise über den Port 1024 initiiert wird, antwortet die entsprechende Internet-Seite über den definierten Port 80. Für den Aufruf einer neuen Seite wird dann z.B. der Port 1036 verwendet, d.h., mit jedem neuen Seitenaufruf wird ein neuer, höherer Port verwendet, was nach längerem Surfen bis hin zu einem Port 13xx führt. Die Ports werden zwar wieder geschlossen, gleichwohl werden erst dann wieder niedrigere Ports (1024) verwendet, wenn der Internet-Explorer beendet und (nach einiger Zeit) neu gestartet wird.

Inhalt des Skriptes mstbridge.sh:

```
# ----- mstbridge.sh -----
# Bridge-Initialisierung, 20.6.04. K. Dembowski
# Hilfetexte durch brctl -help
# Aktivierung der Bridge durch Aufruf von mstbridge.sh
# Deaktivierung mit: ifconfig mstbridge down
# Konfigurierung der Firewall mit iptable-Regeln
echo "Bridge wird gestartet"
echo " "
brctl addbr mstbridge      # Anlegen der Bridge mstbridge
brctl addif mstbridge eth0
        # Netzwerk-Interface 1, LAN-Anschluss 1 (extern)
brctl addif mstbridge eth1
        # Netzwerk-Interface 2, LAN-Anschluss 2 (intern)
```

Firewalls

```
# Für die Bridge-Funktion macht es keinen Unterschied, was als # intern und was als  
extern konfiguriert wird !
```

```
ifconfig mstbridge up      # Starten der Bridge  
brctl show                 # Anzeige der Bridge-Einstellungen
```

```
# ----- Regelsatz fuer die Firewall -----
```

```
iptables -F FORWARD      # Alle Regeln loeschen  
iptables -P FORWARD DROP # Alles verbieten (default policy)
```

```
# Ungueltige Pakete abweisen (kurzer Header, illegale Flags)  
iptables -A FORWARD -m unclean -j DROP
```

```
# Pakete von gefaelschten (ungueltigen, privaten, Loopback)  
# Adressen abweisen  
iptables -A FORWARD -s 192.168.0.0/16 -j DROP  
iptables -A FORWARD -s 172.16.0.0/12 -j DROP  
iptables -A FORWARD -s 127.0.0.0/8 -j DROP  
iptables -A FORWARD -s 10.0.0.0/8 -j DROP
```

```
# Verkehr zu bestimmten IP-Adressen verbieten  
iptables -A FORWARD -d 64.245.58.28 -j DROP # Audio Galaxy  
iptables -A FORWARD -d 209.139.200.43 -j DROP # E-Donkey
```

```
# Obere Ports explizit verbieten  
iptables -A FORWARD -i eth0 -p UDP --dport 1400:65535 -j DROP  
iptables -A FORWARD -i eth1 -p UDP --sport 1400:65535 -j DROP  
iptables -A FORWARD -i eth0 -p TCP --dport 1400:65535 -j DROP  
iptables -A FORWARD -i eth1 -p TCP --sport 1400:65535 -j DROP
```

```
# Verkehr von innen (eth1) nach aussen (eth0) erlauben  
# Alle Protokolle, alle Ports, aber nur aus dem internen Netz  
# Interfaces (eth) muessen nicht mit angegeben werden, mit Angabe # wird es aber  
deutlicher  
iptables -A FORWARD -i eth1 -o eth0 -s 134.28.56.0/24 -j ACCEPT
```

```
# Verkehr von aussen (eth0) nach innen (eth1) erlauben  
# Erlaubt nur Pakete fuer bereits bestehende Verbindungen  
# (ESTABLISHED) und was logisch zu einer Verbindung gehoert  
# (RELATED)  
iptables -A FORWARD -i eth0 -o eth1 -m state -state  
ESTABLISHED,RELATED -j ACCEPT
```

```
# Logging abgewiesener Pakete, steht in /var/log/messages  
# 2 Pakete pro Minute protokollieren, maximal 2 Treffer intern # bearbeiten
```

```
# Abgelehnten Paketen den Text ABGEWIESEN voranstellen
iptables -A FORWARD -m limit --limit 2/minute --limit-burst 2 -j LOG --log-level
notice --log-prefix "!ABGEWIESEN:"
```

Aus Sicherheitsgründen sollten auf dem Bridge-Firewall-PC keine Anwendungen wie Samba, http, FTP, Telnet und dergleichen installiert werden, sondern lediglich das absolut Notwendige.

Das Bridge-Skript (mit iptables) wird beim Start des PC automatisch geladen. Damit dies funktioniert, befindet sich in dem Verzeichnis, wo sich alle automatischen Skripte befinden (*/etc/init.d/*), die Datei *bridgefw*. Der Link (*@S30bridgefw*) hierauf ist unter *etc/init.d/rc3.d* lokalisiert, wo alle Module für den Run-Level-3 abgelegt sind.

Als Log-File für die abgewiesenen Pakete wird nicht mehr *Messages*, wo alle möglichen Meldungen landen, sondern ein File unter *var/log/firewall* verwendet. Unter *etc/logfiles* ist die maximale Größe der Firewall-Log-Datei auf 4 MByte begrenzt, und diese wird täglich (cron-Funktion) gelöscht. Die laufende Anzeige der abgewiesenen Pakete lässt sich mit *tail -f /var/log/firewall* auslösen.

16.2.3 Securepoint Firewall

In diesem Kapitel wird auf eine kommerziell erhältliche Firewall der Firma Securepoint eingegangen. Bei ihr handelt es sich um ein System mit der Bezeichnung *Unified Threat Management (UTM)*, dessen Ziel es ist, an einem zentralen Punkt Sicherheit für das gesamte Netzwerk einer Organisation zu schaffen, was über die alleinige Funktion einer Firewall, wie es zuvor beschrieben wurde, hinausgeht.

Aus dem Kapitel 16.1 ist sicher deutlich geworden, dass es mit viel Arbeit verbunden sein kann, alle einzelnen PCs sicherheitstechnisch abzusichern und auf aktuellem Stand zu halten, so dass sich eine zentrale Lösung bereits bei relativ wenigen PCs im LAN bezahlt machen kann.

Die vorherigen Kapitel haben außerdem gezeigt, dass mit Linux zwar kostengünstige Firewall-Systeme im Selbstbau zu realisieren sind, dieses jedoch einiges an Linux-Erfahrung nicht nur bei der Konfiguration selbst, sondern auch im laufenden Betrieb, etwa für die Änderung der Paketregeln, erfordert.

Spätestens, wenn neben der eigentlichen Firewall-Funktion noch weitere Sicherheitsmechanismen wie für Virensan und die Unterstützung von VPNs nötig werden, ist man an einem Punkt angelangt, an dem ein Gesamtsystem mit zentraler Administrationsmöglichkeit für die Abdeckung möglichst aller relevanten Gefahrenquellen wünschenswert ist, was dann zu einem *Unified Threat Management System (UTM)* führt. Voraussetzung für die Bezeichnung als UTM ist eine Funktionskombination bestehend aus:

- ▶ Firewall (Stateful Inspection, Proxy)
- ▶ Intrusion Detection System (IDS/IPS)
- ▶ Internet-Gateway (Router, Modem, DSL)
- ▶ Virusscanner (HTTP, FTP, POP3, SMTP)

- ▶ Spam-Filter (SMTP, POP3)
- ▶ Content-Filter (Kategorien, Antivirus, File Extension Blocking)
- ▶ Authentisierungs-Mechanismen (RADIUS, Userdatenbank, SPUVA)
- ▶ Virtual Private Network (VPN) Gateway (PPTP, L2TP, IPSec)
- ▶ Reporting- und Logging-Funktionen (Surfverhalten, Statistik Einbruchsversuche, Benachrichtigung)
- ▶ Quality of Service (QoS)
- ▶ Zusätzlich: DHCP-Server, DNS Relay (LAN/WAN), DynDNS-Support

Die Firma Securepoint bietet die UTM-Software separat und auch fertig installiert und vorkonfiguriert mit passender Hardware (Appliances) an.

Das Interessante ist, dass sich die komplette Software auf einer Seite der zum Buch mitgelieferten CD befindet, die uneingeschränkt für den privaten Gebrauch nutzbar ist. Es gibt gegenüber der käuflichen Version nur keinen Support und keine Updates.

Dem Leser ist es also gestattet, mit der Software eine eigene Netzwerk-Firewall aufzubauen, wofür auch ein etwas älterer PC verwendet werden kann, sofern er mindestens über zwei Netzwerkkarten verfügt. Wenn eine DMZ realisiert werden soll, ist mindestens noch eine weitere Netzwerkkarte notwendig.



CD 2 enthält das komplette *Unified Threat Management System* der Firma Securepoint. Die Software darf zum Aufbau einer eigenen Firewall verwendet werden, wofür sich auch ein etwas älterer PC eignet.

Die Firewall kombiniert das Prinzip der Stateful Inspection (Kapitel 16.2) mit verschiedenen Application Proxies (HTTP, POP3, VNC, VoIP). Ergänzt wird sie durch ein *Intrusion Detection System* (IDS) zur Erkennung von Angriffen, die sich typischerweise durch Anomalien (ungültige Pakete, falsche Adressen, vgl. Listung der Bridge Firewall), d.h. Abweichungen vom RFC-Standard, auszeichnen. Das implementierte IDS schützt somit vor Portscans und DoS-Attacken, wobei nicht nur ein Alarm beim Auftreten ausgelöst wird, sondern die entsprechenden Pakete automatisch verworfen werden, was dann als *Intrusion Prevention System* (IPS) bezeichnet wird.

Systemvoraussetzungen

Die Hardware-Anforderungen an den PC, der die Netzwerk-Firewall bilden soll, sind eher gering, wobei es natürlich auch davon abhängt, für wie viele PCs und mit welchen zusätzlichen Diensten (Virus Check, Content Filter etc.) die Firewall arbeiten soll. Je mehr PCs und Funktionen dies sind, desto leistungsfähiger muss der PC sein, wobei in den Securepoint-Appliances unterschiedliche Prozessoren vom Typ VIA-C3 bis hin zu aktuellen Dual Core- und XEON-CPU's von Intel zum Einsatz kommen.

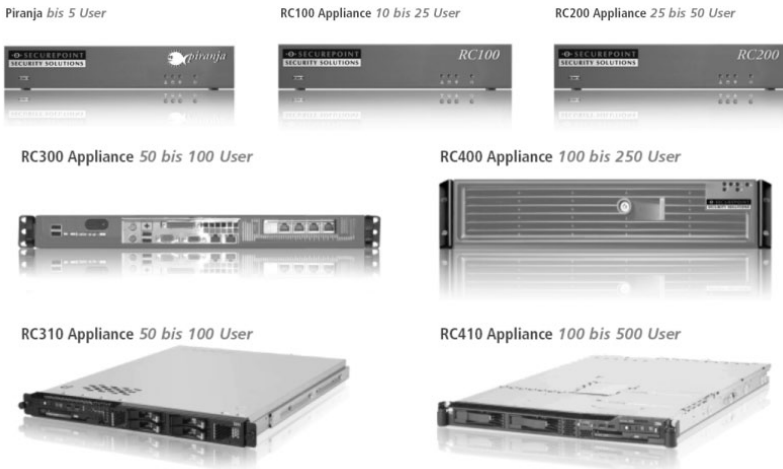


Abbildung 16.11: Appliances der Firma Securepoint

Für eine Probeinstallation und ein kleines LAN bis zu 10 PCs reicht ein Pentium III mit 128 MByte, einer 10 GByte Festplatte sowie einem CD-ROM-Laufwerk (Abbildung 16.12) aus. Auf der beiliegenden Securepoint-CD (CD2) sind genauere Angaben (Whitepapers Hardware Guide) zur geeigneten Hardware zu finden, wobei ein besonderes Augenmerk auf die unterstützten Netzwerkadapter zu richten ist, denn ohne die ist natürlich keine Netzwerk-Firewall zu realisieren.

Die Securepoint-Software besteht aus zwei wesentlichen Teilen: Der eine Teil arbeitet direkt auf der Firewall und der andere auf einem Windows-PC, der für die Konfiguration verwendet wird. Die Installation der Firewall-Software (auf der Appliance) erfolgt vollautomatisch, indem von der mitgelieferten CD aus gebootet wird. Hierfür sind keinerlei manuelle Einstellungen oder sonstige Arbeiten des Anwenders erforderlich. Die möglicherweise auf dem PC vorhandene Software ist danach komplett gelöscht, denn die Festplatte wird zunächst formatiert, so dass auch keine Multiboot-Funktion vorgesehen ist, d.h., auf der Festplatte des Firewall-PC befindet sich nach Fertigstellung ausschließlich die Securepoint-Software.

Dabei handelt es sich um eine spezielle, an die Funktion eines Unified Threat Management-Systems angepasste Linux-Version mit aktuellem Kernel. Für den Anwender und auch für den Administrator des Systems spielt diese Software jedoch keine Rolle, weil er nie direkten Kontakt mit ihr hat – was auch gar nicht vorgesehen ist – und deshalb über keinerlei Linux-Kenntnisse verfügen muss.



Abbildung 16.12: Dieser ältere PC (Pentium III, 450 MHz) mit drei Netzwerkkarten ist ideal für eine Securepoint-Firewall, die ein kleines LAN absichern soll.

Nach der automatischen Installation der Software auf der Appliance kann dieses System gewissermaßen als *Black Box* betrachtet werden, und es sind nur noch die beiden Netzwerkkarten anzuschließen. Die Zuordnung und die Voreinstellungen sind dabei wie folgt:

- ▶ **eth0**: erste Netzwerkkarte, zum Internet, ohne IP-Adresse
- ▶ **eth1**: zweite Netzwerkkarte, zum LAN, mit 192.168.175.1 als IP-Adresse
- ▶ **eth2**: dritte (optionale) Netzwerkkarte für die DMZ, ohne IP-Adresse

Die Software ist zwar auf der Festplatte installiert, allerdings läuft sie komplett im RAM ab, wofür im Speicher eine RAM-Disk eingerichtet wird. Aus diesem Grunde kann die Appliance einfach, ohne herunterzufahren, ausgeschaltet werden, Spannungsausfälle bleiben ohne Auswirkungen und Beschädigungen am Dateisystem oder auch Software-Manipulationen kann es nicht geben. Deshalb profitiert die Appliance von einem möglichst großen RAM-Speicher, während der Prozessortyp weniger wichtig ist. Die Securepoint-Appliances verfügen über einen Speicher von 256 MByte beim kleinsten Modell bis hin zu 2 GByte beim leistungsfähigsten.

Für den Einsatz des Firewall-Systems als Black Box, also ohne Monitor, Tastatur und Maus, ist zu beachten, dass der PC ohne eine angeschlossene Tastatur booten können muss. Im BIOS-Setup lässt sich meist bestimmen, ob der PC bei der Feststellung eines (vermeintlichen) Fehlers wie dem Fehlen einer Tastatur (Boot on Error: All but Keyboard) weiter booten soll oder nicht.

Installation

Nach dem Einlegen der CD in das optische Laufwerk der Appliance wird von dieser gebootet, und es erscheint eine Startseite, wo mit der Pfeiltaste auf *Install* zu navigieren ist, damit die (Linux-)Software daraufhin installiert wird. Alternativ besteht auch die Möglichkeit, ein Image für einen USB-Speicherstick anzufertigen, um dann von dort aus zu booten, falls kein optisches Laufwerk für die Installation der Appliance-Software zur Verfügung stehen sollte.

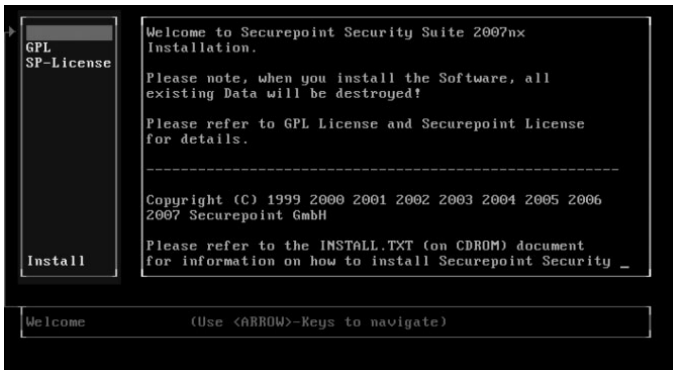


Abbildung 16.13: Nach der Auswahl von Install wird die Appliance-Software ohne weitere Rückfragen installiert.

Nach wenigen Minuten erscheint nach erfolgreicher Installation ein Login, der mit *admin* und dem Passwort *insecure* zu bestätigen ist. Daraufhin wird die Installation zu Ende geführt, und die Anzeige *firewall.foo.local>* signalisiert, dass die Appliance nun für die Konfigurierung zur Verfügung steht.

Die Konfigurierung des Systems erfolgt mithilfe eines Windows-PC, der sich (zunächst) im gleichen Netz (192.168.175.xxx) wie die Appliance befinden muss, die standardmäßig die IP-Adresse 192.168.175.1 besitzt.

Wie üblich, sollte ein Ping an diese Adresse zu einer Antwort führen, und die LEDs an den Netzwerkkarten können den entsprechenden Verbindungsstatus visualisieren, so dass soweit alles in Ordnung ist und die Securepoint-Software installiert werden kann.



Abbildung 16.14: Die Securepoint-Software für Windows stellt ein umfassendes Paket für ein UTM-System dar.

Die Software ist recht benutzerfreundlich aufgebaut und bietet neben den beiden grundlegenden Installations-/Konfigurations- und Management-Tools (Security Wizard, Security Manager) zusätzliche Software wie einen SSH- und VPN-Client, einen Log-Server für die Aufzeichnung der Firewall-Ereignisse, ein Imaging-Tool für die Anfertigung eines bootfähigen USB-Sticks und eine ausführliche Dokumentation zu allen möglichen Optionen, die das *Unified Threat Management System* bietet.

Für die Benutzung der Securepoint-Software eignet sich jeder übliche PC mit Windows 2000, XP oder Vista, mit Windows 98 funktioniert sie nicht. Die Daten zwischen dem Windows-PC und der Appliance werden per SSH verschlüsselt auf dem Port 22 übertragen.

Security Wizard

Da der *Securepoint Security Wizard* für die grundlegende Konfigurierung des Systems vorgesehen ist, wird er zuerst installiert und aufgerufen. Der Wizard ermöglicht die menügeführte, schrittweise Erstellung einer UTM-Systemkonfiguration, und durch die Bearbeitung der einzelnen Punkte ist ein mit den Basiseinstellungen funktionsfähiges System recht schnell realisiert.

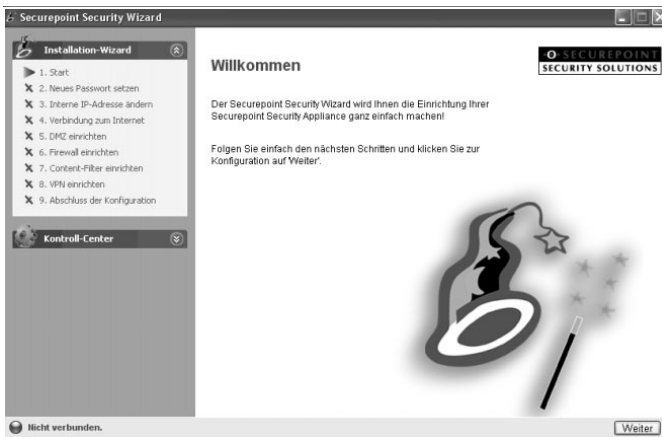


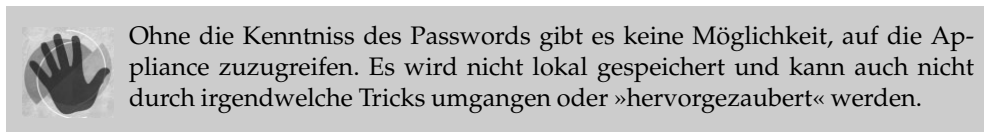
Abbildung 16.15: Der Installation Wizard hat nach neun Schritten das System grundlegend konfiguriert.

Nach der Anerkennung der Nutzungsbedingungen und der Eingabe der Benutzerdaten führt der Wizard durch die folgenden Installationsschritte. Stellt er während des Konfigurationsvorgangs fest, dass bereits ein vollständiger Durchlauf stattgefunden hat, beendet er die Arbeit und verweist auf die Benutzung des Kontroll-Centers. Dieses wird über den Wizard aufgerufen und bildet mit ihm zusammen den Dreh- und Angelpunkt für die grundlegende Konfigurierung des UTM-Systems.

Es kann natürlich der Fall eintreten, dass ein absolvierter Konfigurationsvorgang nicht zu einem funktionierenden System geführt hat und darauf folgende manuelle Einstellungen die Appliance völlig »verkonfiguriert« haben. In solch einem Fall sei dem Einsteiger empfohlen, eine erneute Installation der Linux-Appliance-Software mit anschließendem Wizard-Durchlauf auszuführen.

Außer dem Wizard gibt es den *Security Manager*, der über die Möglichkeiten, die im Kontroll-Center zu finden sind, weit hinausgeht und eine Vielzahl von Einstellungsmöglichkeiten bietet, mit denen das System bis in letzte Detail ausgenutzt werden kann. Für den Einstieg erscheint es möglicherweise als zu komplex, so dass das Kontroll-Center zunächst zu bevorzugen ist.

Im zweiten Wizard-Schritt wird das Password für den Zugriff auf die Appliance festgelegt, wobei es bestimmten Kriterien (vgl. auch Kapitel 13.2.6) hinsichtlich der Verwendung von Zahlen, Zeichen sowie Groß- und Kleinschreibung entsprechen muss, damit es vom System akzeptiert wird. Von der Alternative, das Password stattdessen durch das System generieren zu lassen, sollte eher kein Gebrauch gemacht werden, weil dies eine zufällige Kombination ergibt, die man sich kaum merken kann. Da beim späteren Zugriff auf die Appliance das Password anzugeben ist, sollte dieser Schritt mit Bedacht ausgeführt werden.



Nicht selten wird das generierte Password vor lauter Begeisterung darüber, dass die angelegte Konfiguration sofort funktioniert, was wiederum zum weiteren Ausprobieren verleitet, nicht notiert, so dass ein erneuter Zugriff dann nicht mehr möglich ist.

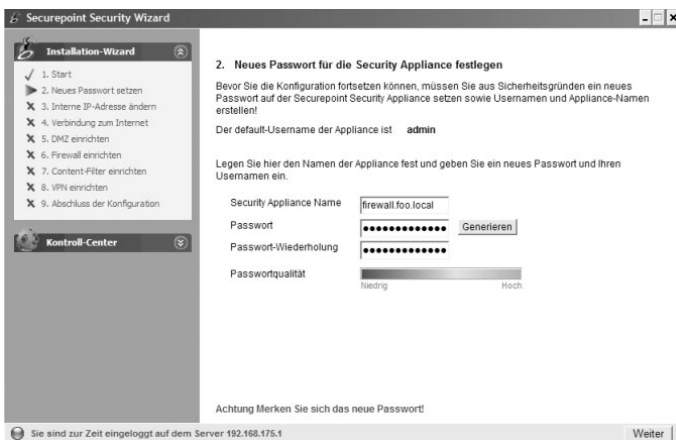


Abbildung 16.16: Das Password sollte selbst bestimmt werden, wobei die Konfigurierung nur dann fortgesetzt werden kann, wenn es eine bestimmte Qualität aufweist.

Im dritten Schritt wird die IP-Adresse der Appliance festgelegt, was möglicherweise eine vorübergehende Veränderung der IP-Adresse bei dem PC zur Folge hat, mit dem gerade die Konfigurierung vorgenommen wird. Der Wizard führt jedoch auch hierfür die notwendigen Schritte aus und meldet den Erfolg der Umstellung mit den jeweiligen Adressen, so dass die getroffene Einstellung noch einmal bestätigt wird.

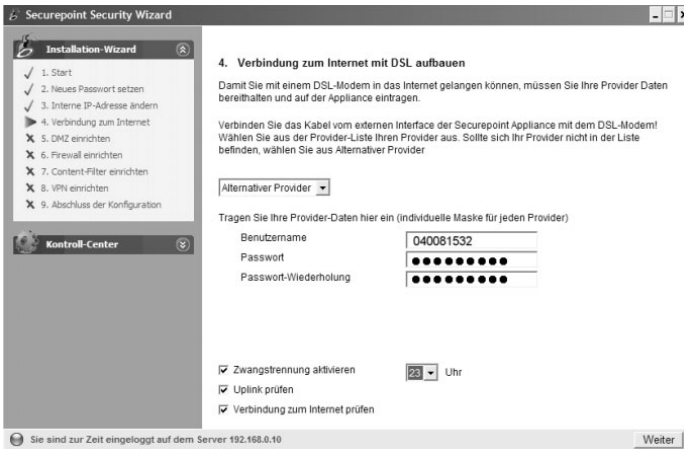


Abbildung 16.17: Der Internetzugang soll über ein DSL-Modem erfolgen.

Der nächste Schritt bestimmt die Art des Internetzugangs, wobei es hierfür die Optionen ZUGANG ÜBER EIN DSL-MODEM ODER ÄHNLICHES gibt, womit dementsprechend auch ein anderes Modem (analoges, Kabelmodem) gemeint sein kann, und INTERNETZUGANG ÜBER EINEN ROUTER. In der Abbildung 16.17 ist die Konfigurationsseite für die erste Option gezeigt, wobei einige Provider hier bereits voreingestellt sind. Falls der gewünschte nicht dabei ist, wird hier *Alternativer Provider* gewählt, und die entsprechenden Zugangsdaten werden eingegeben. Bei dieser Gelegenheit sollte auf dieser Seite auch gleich die Internetverbindung überprüft werden, und optional kann eine Uhrzeit für die automatische Trennung bestimmt werden.



Das ADSL-Modem sollte vor dem Einschalten der Appliance bereits aktiviert sein, d.h. über einen ADSL-Link verfügen, was auch für den späteren Betrieb gilt, weil andernfalls nicht sichergestellt werden kann, dass eine Internet-Verbindung zustande kommt.

Außerdem kann bei Bedarf in diesem Schritt auf der darauf folgenden Seite der DynDNS-Internetdienst aktiviert werden, der dafür sorgt, dass der DSL-Zugang trotz wechselnder IP-Adresse, die vom Provider zugeteilt wird, stets über den gleichen Hostnamen (DNS) erreichbar ist. DynDNS setzt eine entsprechende Registrierung bei www.dyndns.org voraus.

Ebenfalls optional ist die Einrichtung einer DMZ, so dass im sechsten Schritt die Firewall eingerichtet werden kann. An dieser Stelle ist alles, was nicht explizit erlaubt ist, verboten. Typischerweise wird man zunächst http sowie DNS für das Internet erlauben. Alles (any) zu erlauben, empfiehlt sich wie die Freischaltung von Ping nur für Testzwecke, zumal sich die externe Adresse bei der Verwendung eines Modems ohnehin des Öfteren ändert.

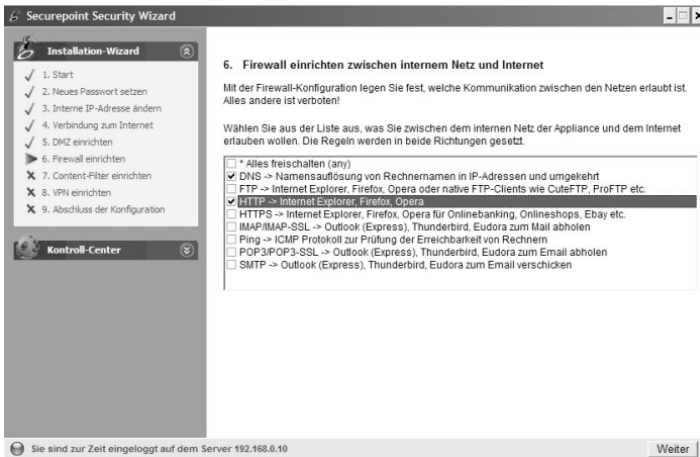


Abbildung 16.18: Das Einrichten der Firewall

Nach der Einrichtung der Firewall schließt sich die des Content-Filters an, wo zunächst Begriffe wie violence, discrimination oder pornography aktiviert werden können, was zur Sperrung der diese Begriffe enthaltenen Internetseiten führt. An dieser Stelle alles Mögliche anzuklicken, was verboten sein soll, wie etwa auch file-extensions, chat, forums, führt nicht selten dazu, dass auch Seiten gesperrt werden, die man eigentlich gar nicht »im Visier« hatte, so dass es empfehlenswerter ist, sich an die passenden Einstellungen heranzuarbeiten, wofür eine Analyse der Logging-Daten nützlich sein kann. Die Aktivierung von File-Extensions führt im Übrigen dazu, dass Google oder auch MSN nicht mehr erlaubt sind (Abbildung 16.22).

Die zweite Seite des Content-Filters führt Extensions (arj, bat, com, exe...) von Dateien bzw. Programmen auf, die ebenfalls blockiert werden sollen, was gegenüber der ersten Content-Filterseite zu eindeutigen Ergebnissen führt.

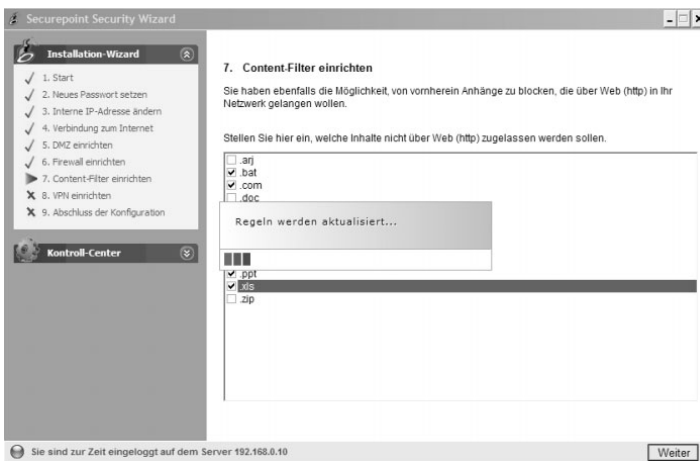


Abbildung 16.19: Nach der Einrichtung des Content-Filters werden die bisherigen Festlegungen für die Appliance aktualisiert.

Als vorletzter Schritt kann noch ein VPN eingerichtet werden, was bei Bedarf auch später nachgeholt werden kann und deshalb bei dieser grundlegenden Konfiguration nicht betrachtet wird.

Daraufhin folgt bereits der Abschluss der Konfiguration, und die kompletten Daten werden über den Button KONFIGURATION AUF DER FIREWALL SICHERN auf die Appliance geschrieben. Nach der Anmeldung am System wird das Kontroll-Center gestartet, welches zunächst die zuvor festgelegten Regeln (Abbildung 16.20) anzeigt.

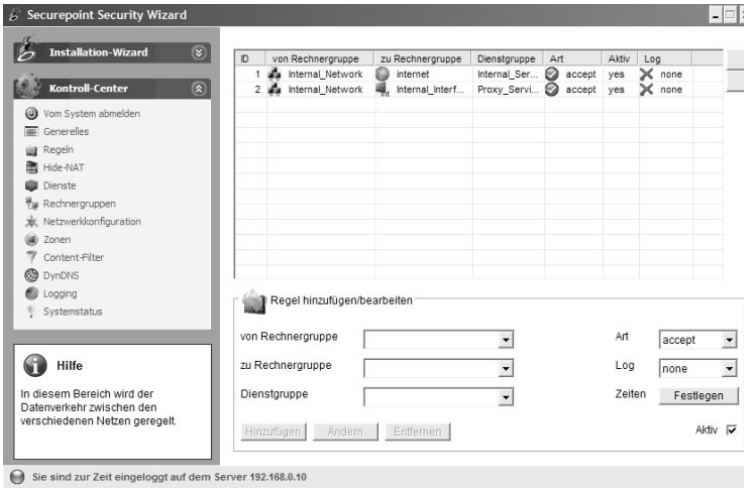


Abbildung 16.20: Nach dem Abschluss der Konfiguration und der Anmeldung am System werden die bisher festgelegten Regeln angezeigt.

Bevor mit dem Kontroll-Center weitere Einstellungen vorgenommen werden, ist zunächst zu überprüfen, ob die festgelegten Regeln auch wie gewünscht funktionieren.

Funktionstest

Um die Verbindung zum Internet herstellen zu können, ist mit den Standardeinstellungen die Eintragung eines Proxy notwendig, was beim Internet Explorer über EXTRAS – INTERNET-VERBINDUNGEN – EINSTELLUNGEN – PROXYSERVER erfolgt. Als Adresse ist hier die Adresse der Appliance zum internen Netz hin anzugeben mit 8080 als Kommunikationsport.

Im Security Manager kann der HTTP-Proxy auf *transparent* geschaltet werden, so dass bei den Browser-Einstellungen dann keine Anpassung notwendig ist und die Benutzer keine Kenntnis von der Proxy-Funktion erhalten.

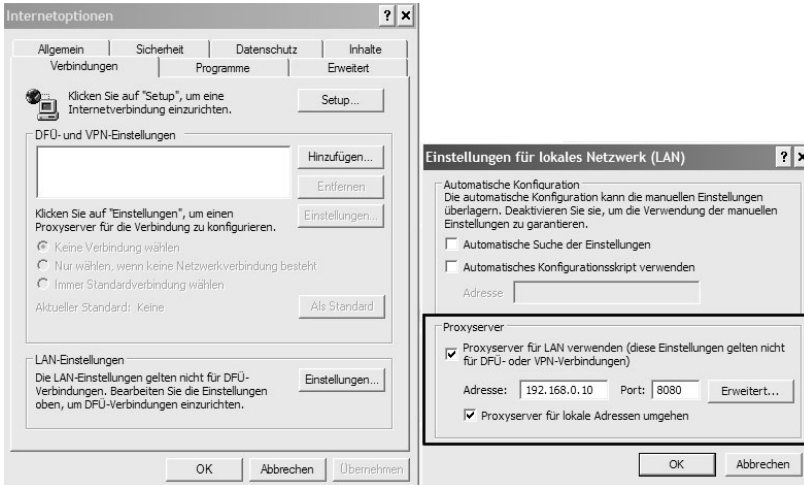


Abbildung 16.21: Damit die Internet-Kommunikation über die Firewall funktioniert, ist sie beim Browser als Proxyserver anzugeben.

Damit sollte der Internetverkehr funktionieren, und wie die Content-Filter greifen, wird dabei auch festgestellt werden können. Meistens bedürfen sie noch der Anpassung, was wie alle weiteren Einstellungen im Kontroll-Center vorgenommen werden kann. Mit dem Security Manager lassen sich Änderungen an den bestehenden Kategorien vornehmen oder auch neue einführen, worauf am Ende des Kapitels noch kurz eingegangen wird.



Abbildung 16.22: Der Zugriff auf Google wird aufgrund (zu) strenger Content-Einstellungen unterbunden.

Logging

Für die Analyse des Datenverkehrs gibt es im Kontroll-Center die Option *Logging*, womit in einem Fenster (Abbildung 16.23) die aktuellen Verbindungsaktivitäten sichtbar gemacht werden. Diese können an dieser Stelle nach bestimmten Mustern (Zeit, Dienst) sortiert und auch in eine Datei geschrieben werden. Mit jedem Aufruf wird ein neues Logging-Fenster eröffnet, so dass vorherige Daten nicht eingesehen werden können.

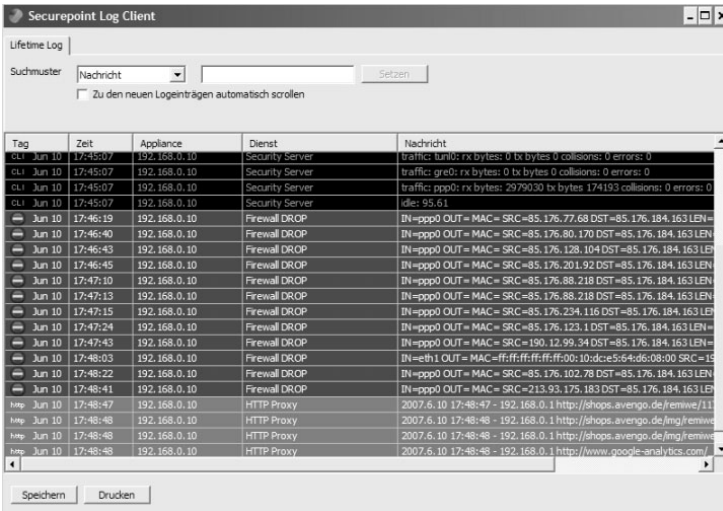


Abbildung 16.23: Im Kontroll-Center gibt es ein temporäres Logging.

Für automatische Aufzeichnungen mit zahlreichen Verwaltungsoptionen wird als Software (Abbildung 16.14) ein separater Log-Server mitgeliefert, der am besten auf einem Windows-Server installiert wird, welcher dann im Dauerbetrieb die Daten von der Appliance empfangen kann. Nach der Installation arbeitet er als Windows-Dienst im Hintergrund. Für die Appliance wird der Log-Server mit dem *Security Manager* festgelegt.

Die Kommunikation zwischen dem Log-Server und der Appliance findet über das standardisierte Syslog-Protokoll (RFC 3164, 3195) statt, so dass die Appliance-Daten auch mit anderen Syslog-Systemen ausgewertet werden könnten. Der Log-Server führt eine Datenbank und kann per Email regelmäßige Reports an den Administrator schicken sowie bei Einbruchversuchen eine entsprechende Nachricht generieren.

Authentisierung

Für die Authentisierung, damit beispielsweise nur entsprechend ausgewiesene Benutzer das Internet benutzen und Emails abrufen können, sind verschiedene Methoden anwendbar, wobei dies am einfachsten per RADIUS-Server (Remote Authentication Dial-In User Service) in einer Windows Server 2003-Umgebung, eben ohne das Anlegen neuer Benutzer, funktioniert.

Hierfür muss auf dem Windows Server der Internetauthentifizierungsdienst (IAS) installiert und im Active Directory bekannt gemacht sowie die Securepoint Appliance als Client hinzugefügt werden. Ein entsprechendes How-to, welches sich wie die gesamte Securepoint-Dokumentationen auf der CD befindet, beschreibt die hierfür notwendige Vorgehensweise ganz genau.

Den Anwendern können mithilfe des *Securepoint User Verification Agent* (SPUVA) individuelle Rechte für ihre Arbeitsplätze im DHCP-Umfeld gegeben werden. Diese authentisieren sich dann über den SPUVA und erhalten ihre vorbestimmten Sicherheitseinstellungen an jedem hierfür vorgesehenen PC-Arbeitsplatz.

Die SPUVA-User werden in einer Gruppe zusammengefasst und als Netzwerkobjekte konfiguriert, wobei die Appliance als SPUVA-Server fungiert. Die Einlog-Zeiten der Benutzer werden automatisch dokumentiert und können für die Arbeitszeiterfassung oder ähnliches weiterverwendet werden. Außerdem können für die Authentisierung noch digitale Zertifikate nach X.509 sowie eine separate interne Datenbank eingesetzt werden, was in allen drei Fällen jedoch neben den standardmäßigen eine »doppelte Buchführung« von Benutzerdaten bzw. -konten bedeutet.

Security Manager

Der Wizard verfügt nur über eine eingeschränkte Funktionalität für die schnelle Konfiguration, während der *Security Manager* das vollwertige Werkzeug für die Konfigurierung des UTM-Systems darstellt.

Bei der Kontaktaufnahme mit der Appliance wird die mit dem Wizard erstellte Konfiguration vom Manager übernommen, so dass die Einstellungen bei Bedarf weitergeführt und optimiert werden können. Es sei jedoch noch einmal explizit darauf hingewiesen, dass die Benutzung des Managers nicht zwingend ist, und falls mit dem Kontroll-Center bereits eine den Wünschen entsprechende Konfiguration hergestellt worden ist, kann auf die Benutzung des Managers auch verzichtet werden.

Beim ersten Start des Security Managers erscheint ein Dialog-Feld für die Erzeugung eines so genannten Containers, wofür ein Schlüssel festzulegen ist. Der Container enthält alle Zugangs- und Konfigurationsdaten in verschlüsselter Form. Bei jedem folgenden Aufruf des Managers ist der festgelegte Schlüssel dann wieder einzugeben, so dass er wie ein Passwort zu behandeln ist.

Danach ist die Appliance dem Manager bekannt zu machen, was durch einen Klick auf das rote Firewall-Symbol eingeleitet wird und mit Angabe der Appliance-IP-Adresse sowie Login mit Password erfolgt. An dieser Stelle (FIREWALL HINZUFÜGEN) kann außerdem der zuvor bereits erwähnte Logserver festgelegt werden. Mit dem Manager lassen sich mehrere Appliances völlig unabhängig voneinander konfigurieren.

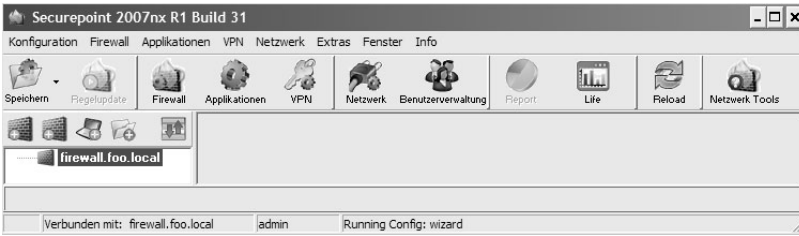


Abbildung 16.24: Der Security Manager ist mit der Firewall verbunden, und es sind noch keine Menüs selektiert.

Im Manager erscheint nach erfolgreicher Einstellung die Bezeichnung der Firewall (firewall.foo.local), und wenn sie daraufhin gefunden wurde, wird die Bezeichnung grün dargestellt. Eine gelbe Markierung bedeutet, dass die Authentisierung anhand des Schlüssels stattgefunden hat und sich die Appliance aktuell im Standby-Modus befindet, während eine rote Markierung besagt, dass die Appliance nicht gefunden wurde, so dass dann keine Konfigurationsmaßnahmen durchgeführt werden können. Wenn 15 Minuten lang keine Daten übertragen wurden, schaltet die Appliance automatisch in den Standby-Modus.

Die Manager-Optionen mögen beim ersten Durchblättern fast »erschlagend« wirken, doch dieser Eindruck täuscht; die Konfigurationsseiten sind lediglich über verschiedene Wege – über die Menüleiste, über Symbole oder auch über Pull-Down-Menüs – erreichbar. Dies ist der Übersichtlichkeit weniger zuträglich, und die Möglichkeit, die Anzeige den Vorlieben des Administrators entsprechend einstellen zu können, wäre vielleicht eine Option für die kommende Version. Dennoch sollten sich die wesentlichen Konfigurationsoptionen bereits aus dem Umgang mit dem Kontroll-Center her erklären.

Um das System optimal an die jeweiligen Bedürfnisse anpassen zu können, wird man trotz der sehr ausführlichen Dokumentation der Firma Securepoint nicht umhin kommen, einiges auszuprobieren. Damit dies keinen unabsichtlichen Verlust von getroffenen – bereits funktionierenden – Einstellungen zur Folge haben kann, sollte die Konfiguration nicht nur des Öfftern auf der Appliance gespeichert, sondern auch auf den Windows-PC exportiert werden, was auch als Backup bei einem Ausfall der Appliance dienlich ist.

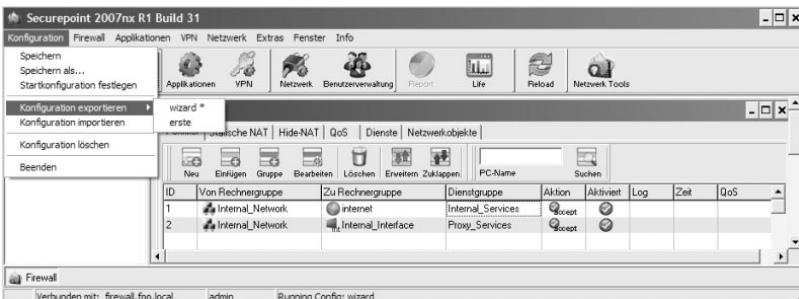


Abbildung 16.25: Speichern und Exportieren der Konfiguration mit dem Security Manager

Die Möglichkeiten, die sich mit dem Security Manager ergeben, sind enorm, was hier natürlich nicht ausführlich behandelt werden kann und auch nicht beabsichtigt ist, weil sich die gelungene Securepoint-Dokumentation auf der CD befindet.

Deshalb wird hier nur noch kurz auf das Erstellen von Firewall-Regeln eingegangen, wofür so genannte *Netzwerkobjekte* von Bedeutung sind, die generell die wesentliche Basis für die individuelle Systemkonfiguration bilden.

Über FIREWALL - PORTFILTER werden zunächst die bereits standardmäßig vorhandenen (und möglicherweise die zuvor per Kontroll-Center erzeugten) Regeln angezeigt. Das Anlegen einer neuen Regel wird hier durch Selektierung von NEU gestartet, wobei eine Regel VON RECHNERGRUPPE über ZU RECHNERGRUPPE mit DIENSTGRUPPE und der jeweiligen AKTION (Accept, Drop, Eject) einfach durch das Selektieren der in diesen vier Menüs vorhandenen Optionen erstellt wird. Für jede Regel kann außerdem bestimmt werden, ob die jeweilige Aktion zur Aufzeichnung führen (Log) und welche Priorität diese Regel gegenüber den anderen erhalten soll, was dann unter QoS festzulegen ist.



Damit neu angelegte Regeln in Kraft treten können, ist im Security Manager der Button REGELUPDATE zu betätigen.

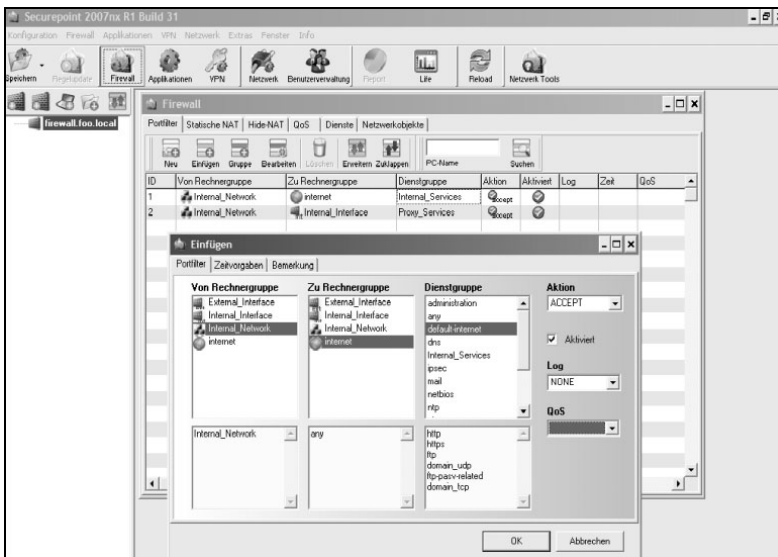


Abbildung 16.26: Das Anlegen einer neuen Regel

Netzwerkobjekte können für Interfaces, Gruppen und Netze auch selbst angelegt werden, falls die standardmäßig vorhandenen nicht passend sein sollten, die jeweils durch Name, IP-Adresse, Maske, Zone und Gruppe ausgewiesen werden.

Dienstgruppen, denen ebenfalls das Prinzip der Objekte zugrunde liegt, lassen sich aus unterschiedlichen Diensten zusammenstellen. In der Abbildung 16.26 ist erkennbar, dass die Dienstgruppe default-internet die einzelnen Dienste http, https, ftp und drei weitere enthält, was unter DIENSTE (Abbildung 16.27) auch noch nach eigenen Wünschen angepasst werden kann.

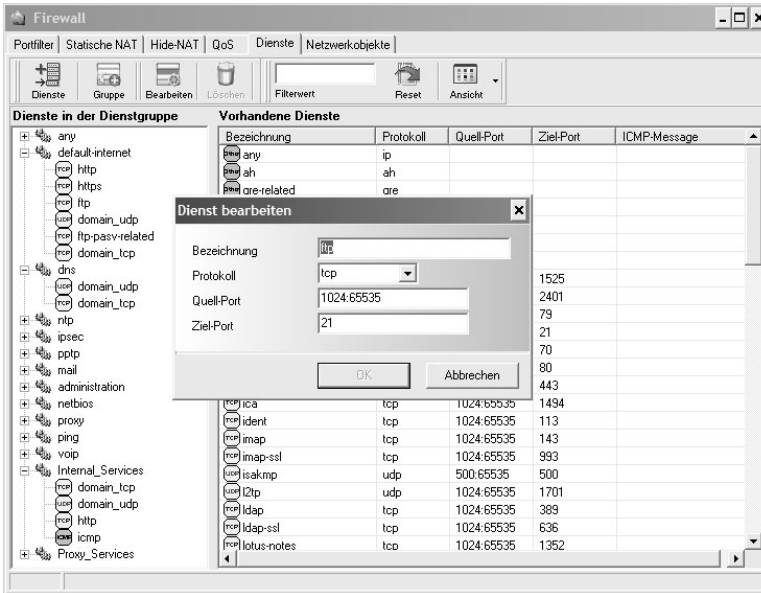


Abbildung 16.27: Die Dienstgruppen enthalten verschiedene Dienste, die in ihren Eigenschaften auch bearbeitet werden können.

Zusammengenommen ergibt sich durch die flexible Objektorganisation eine Vielzahl von Kombinations- und damit Konfigurationsmöglichkeiten, was am besten selbst ausprobiert wird, um einen praktischen Eindruck von der Vielseitigkeit des UTM-Systems zu erhalten.