Firewalls

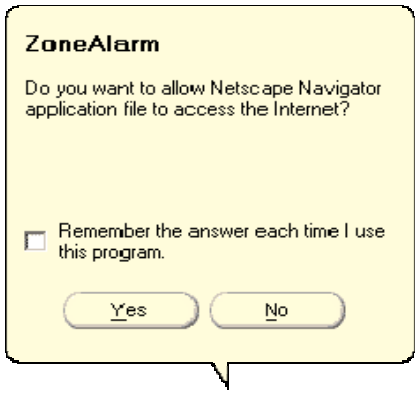
Wozu Firewalls?
Der Einsatz von Firewalls ist eine zuverlässige Methode, den Zugriff von und zu einem System auf das Notwendige zu beschränken. Eine Firewall ist im Grunde genommen eigentlich nichts weiter als ein Filter, der nach definierten Regeln den Zugriff von und zu Rechnern kontrolliert. Eine sehr einfache Firewall blockiert beispielsweise eine Liste von unerwünschten IP-Adressen, die auf das eigene Netzwerk zugreifen dürfen, oder, umgekehrt, eine Liste von Adressen im Internet, auf die von den Netzwerkteilnehmern zugegriffen werden darf. Normalerweise werden in Firmen "richtige" Firewalls eingesetzt, die entweder als Hardware-Lösungen in das Netzwerk implementiert sind oder als Software auf einem eigens dafür vorgesehenen Rechner laufen. Jedoch gilt für eine Firewall immer, egal wie komplex das System sein mag: Der Schutz ist immer nur so gut wie die Regeln, nach denen die Firewall arbeitet.
Für den Heimbedarf gibt es ebenfalls einige Firewalls, die den eigenen PC vor unerwünschten Zugriffen schützen. Einige davon erlauben eine schnelle und einfache Konfiguration, andere wiederum ermöglichen dem Profi detaillierte Einstellungen, welche Programme oder Services über welche **Ports** mit dem Internet kommunizieren dürfen. Diese Ports sind vergleichbar mit Türen, über die die Verbindungen zu einem TCP/IP-Netzwerk geregelt werden. Ein Browser greift in der Regel über den Port 80 auf das Internet zu und sendet und empfängt Daten über diesen Port. Schließt man nun diese Tür, so kann der Browser auch keine Verbindung mehr ins Internet herstellen. Das macht natürlich wenig Sinn, wenn man im Internet surfen will. Interessant wird das erst, wenn außer einem Browser keine andere Anwendung auf einem Rechner existiert, die auf das Internet zugreift. Dann könnte man grundsätzlich alle anderen Türen bis auf den Port 80 schließen und der Rechner wäre gegenüber Attacken geschützt. Ein Trojaner, der sich über den Port 1234 in das Internet verbinden will, hat somit keine Chance, Kontakt zu einem eventuellen Script-Kiddie aufzunehmen.
Das Besondere an diesen Ports ist nun, dass man sie mit einer Firewall entweder für eingehende oder ausgehende Verbindungen blocken kann. Somit wird aus dem Beispiel mit der Tür eine Art Drehkreuz, wie man das z.B. aus dem Zoo oder aus dem Supermarkt kennt. Ein solches Drehkreuz erlaubt das Passieren in nur eine Richtung.
In der Praxis heißt das, dass man seinem Browser den Kontakt zum Internet über den Port 80 erlauben kann, anderen Internet-Teilnehmern jedoch den Zugriff auf den eigenen Rechner über diesen Port verbietet. Stellt man nun solche Regeln für alle Programme wie z.B. Mailprogramme oder Chatprogramme auf, die mit dem Internet kommunizieren dürfen und schließt die restlichen Türen, dann hat man schon ein wirksames Regelwerk für seine Firewall.
Es gibt alleine für Privatanwender unter den Microsoft-Betriebssystemen schon sehr viele Firewalls und das Testen dieser Programme ist eine Wissenschaft für sich. Es handelt sich bei einer Firewall schließlich nicht um eine 08/15-Anwendung wie beispielsweise eine Textverarbeitung oder ein Grafikprogramm, sondern hier laufen viele Vorgänge im Verborgenen ab und sind manchmal nur schwer nachvollziehbar.

ZoneAlarm

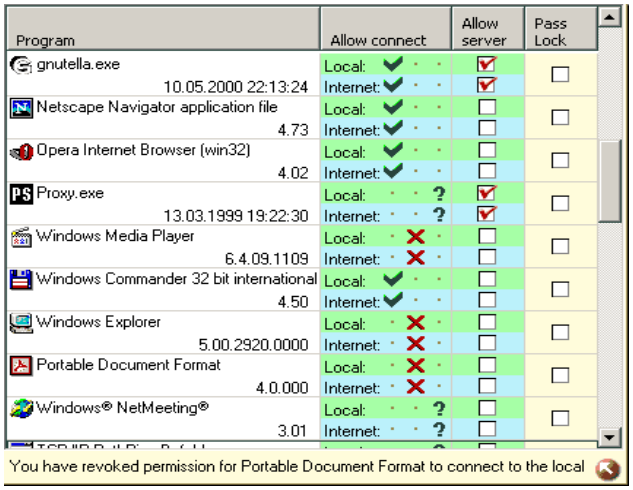
Eine **gratis** erhältliche aber dennoch sehr **effektive** Firewall stellt z.B. ZoneAlarm dar, welche wirkungsvoll ungewünschte Zugriffe von und zu unserem PC blockt. Es ist für Anfänger ein sehr empfehlenswertes Programm das diese Firewall leicht zu bedienen ist.

Man sieht das der Aufbau von ZoneAlarm recht einfach gehalten ist. Neben vier schlichten Balkenanzeigen für den aktuellen Datenverkehr ganz links befinden sich in der Mitte zwei große Schalter, mit denen man Datenübertragungen blocken kann. Der rechte Schalter sieht nach einem dicken Not-Aus-Schalter aus und hat die Funktion, jegliche Kommunikation auf der Stelle zu unterbinden. Etwas weiter rechts davon sieht man die Symbole der Anwendungen, die gerade eine Verbindung ins Netz etablieren wollen. Das kleine Handsymbol unter den Icons symbolisiert, dass die entsprechende Anwendung als Server agieren darf.

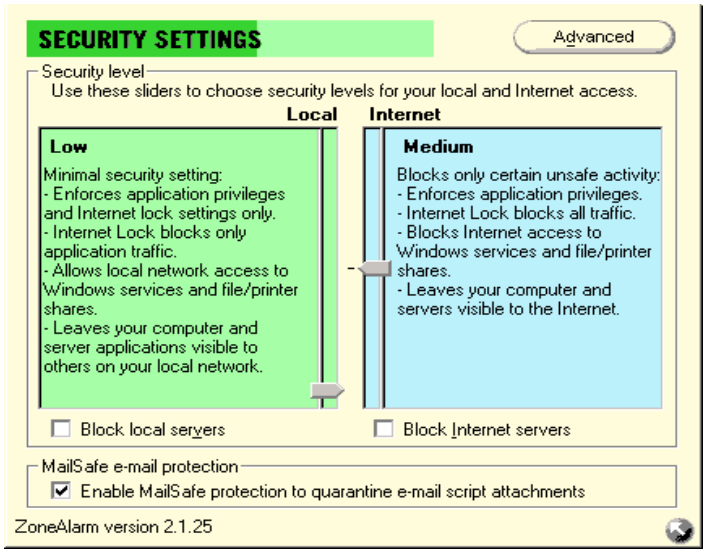
Das Einrichten von ZoneAlarm beschränkt sich auch schon darauf, einfach bei jeder Anwendung, die ins Internet will, diesen Zugriff entweder zu erlauben oder zu verbieten.



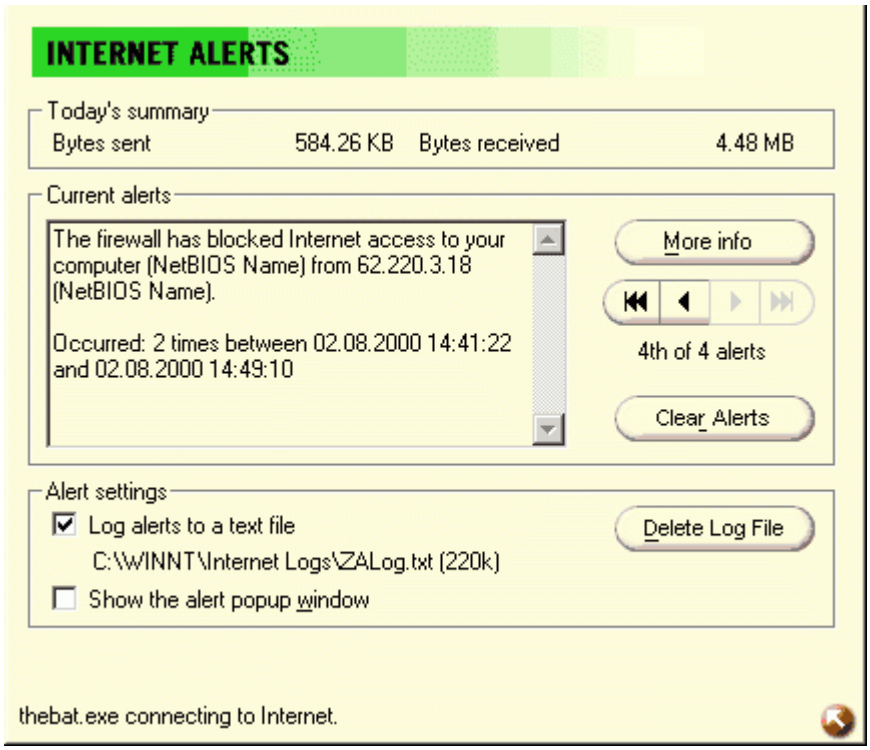
Dabei ist natürlich die Kommunikation durch den Browser, Mail-Clients, Downloadmanager oder Chatprogramme erlaubt, wird keine Kommunikation des Windows Media Players in das Internet erlaubt. ZoneAlarm zeigt die so erstellten Regeln ebenfalls in einer Liste dar, die man selbstverständlich jederzeit ändern kann:



Der Name **ZoneAlarm** kommt daher dass dieses Programm die Teilung in zwei verschiedene Sicherheitszonen erlaubt, nämlich dem **lokalen Netzwerk** und dem **Internet**. Somit lässt sich der Zugriff von Software für die lokale Zone und in der Internet-Zone getrennt einstellen. Die Einstellung nimmt man einfach per Schieberegler vor:



Während man also für das eigene lokale Netzwerk vermutlich die Schieberegler entsprechend niedrig ansetzen kann, sollte man für die Internet-Zone natürlich eine angemessene hohe Sicherheitszone wählen, also mindestens **Medium** oder aber **High Security**, da in dieser Stufe auch die eigenen Ports unsichtbar für andere Internet-Teilnehmer sind. Diese Art Unsichtbarkeit, die sich aus verborgenen Ports ergibt, nennt man übrigens auch **Stealth**.
Auf den ersten Blick entsteht vielleicht der Eindruck, dass es sich bei ZoneAlarm um eine reine Applikationsfirewall handelt, die nur mit Programmen umgehen kann. Jedoch werden von ZoneAlarm ebenfalls auch Zugriffe aus dem Internet abgewehrt, wie man hier anhand der Log-Datei erkennen kann:

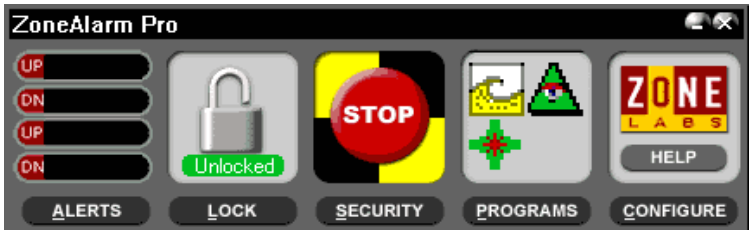


In dem oberen Bild sieht man, dass gleich zweimal ein Zugriffsversuch auf einem Rechner von der IP-Adresse 62.220.3.18 geblockt wurde. Ohne Firewall hätte man diese Attacke nicht einmal mitbekommen und der Teilnehmer hätte je nach seinem Wissensstand eventuell vorhandene Sicherheitslücken auf diesem Rechner ausnutzen können, um heimlich an Daten zu gelangen oder sie zu löschen.

Wie man sieht, sind die Einstellungen von ZoneAlarm recht einfach und unkompliziert zu handhaben. Trotzdem ist dieses Programm meiner Erfahrung nach eine recht zuverlässige Firewall, mit der man sehr effizient die Zugriffe von Applikationen in einem Netzwerk einschränken kann und ist dabei noch sehr unkompliziert zu bedienen. Dass dieses Programm für Privatanwender **kostenlos** erhältlich ist, mindert aber nicht die **Qualität** dieser kleinen Firewall.

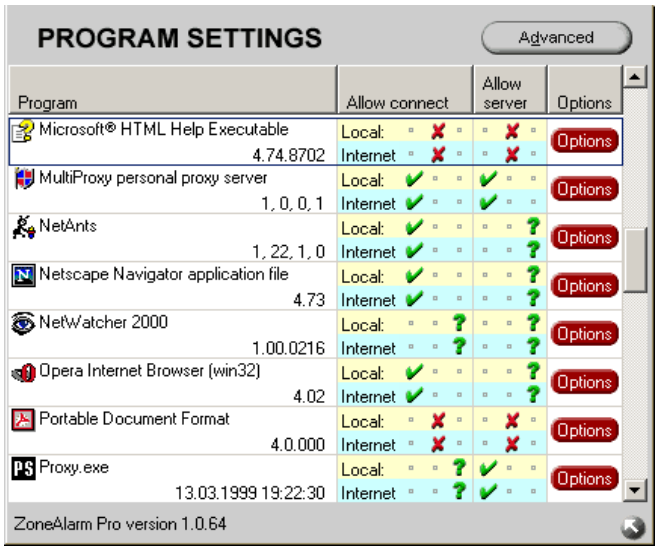
Wem die Fähigkeiten von ZoneAlarm nicht ausreichen oder tiefgreifendere Einstellmöglichkeiten vermisst, für den steht mit Zone Alarm auch eine kommerzielle Version dieses Programms zur Verfügung.

ZoneAlarm Pro
Wer bereits den frei erhältlichen ZoneAlarm kennt, wird sich mit der kommerziellen Version ZoneAlarm Pro sehr schnell zurechtfinden. Gegenüber dem Vorgänger hat sich auf den ersten Blick lediglich das Design verändert.

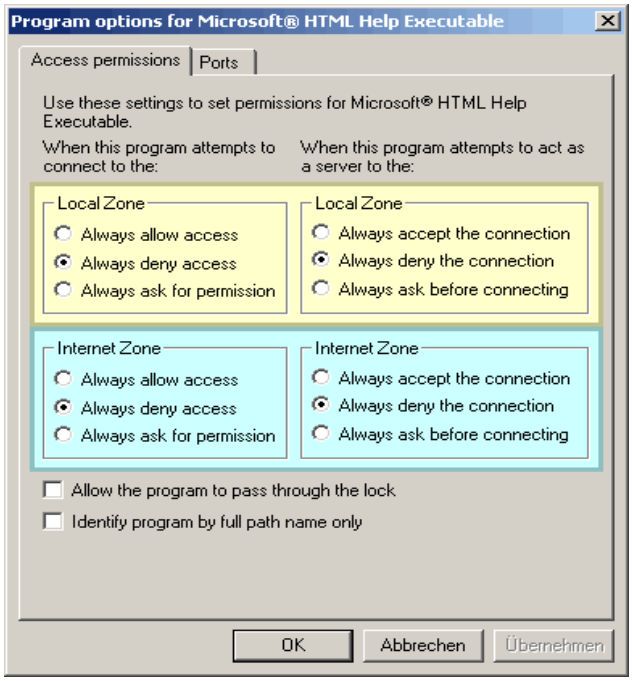


Im Hauptfenster sind alle Symbole noch unverändert vorhanden. Von links nach rechts ist hier ebenfalls die Traffic-Anzeige zu sehen, das Schloss-Symbol zum Sperren des Internet, der "Not-Aus-Schalter", der sofort alle Verbindungen unterbricht sowie die Anzeige, welches Programm sich gerade ins Internet verbinden will.

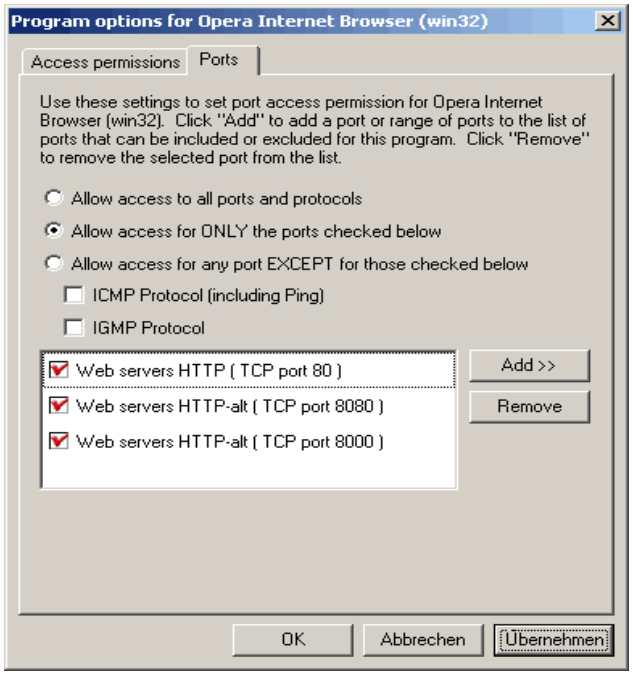
Auch bei ZoneAlarm Pro ist wieder eine Liste der Programme verfügbar, denen man den Zugriff ins Internet erlaubt oder verboten hat. An den grünen Häkchen oder an den roten Kreuzen ist sofort ersichtlich, welches Programm in welche Zone zugreifen darf und ob ein Server-Verhalten erwünscht ist.



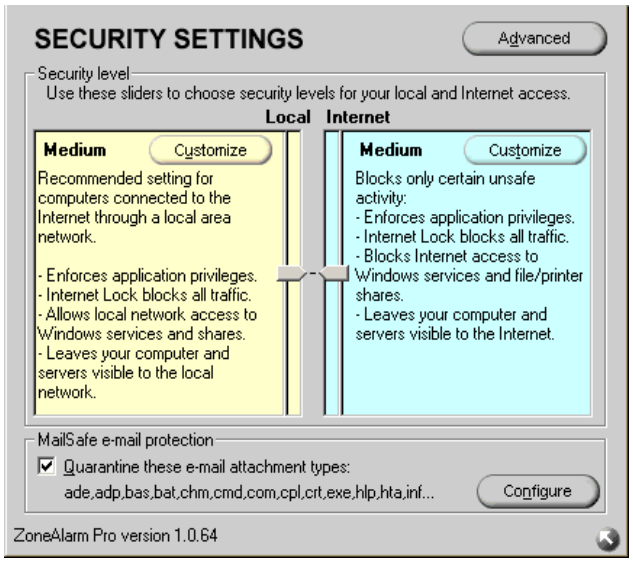
Unter den Options, die für jede Anwendung getrennt konfigurierbar sind, finden sich noch weitere nützliche Einstellmöglichkeiten, wie z.B. die Identifizierung eines Programmes anhand des kompletten Dateipfades, was einen guten Schutz gegen Trojaner ergibt, die sich beispielsweise ja auch iexplore.exe nennen könnten, was in der Regel die Programmdatei des Internet Explorers ist.



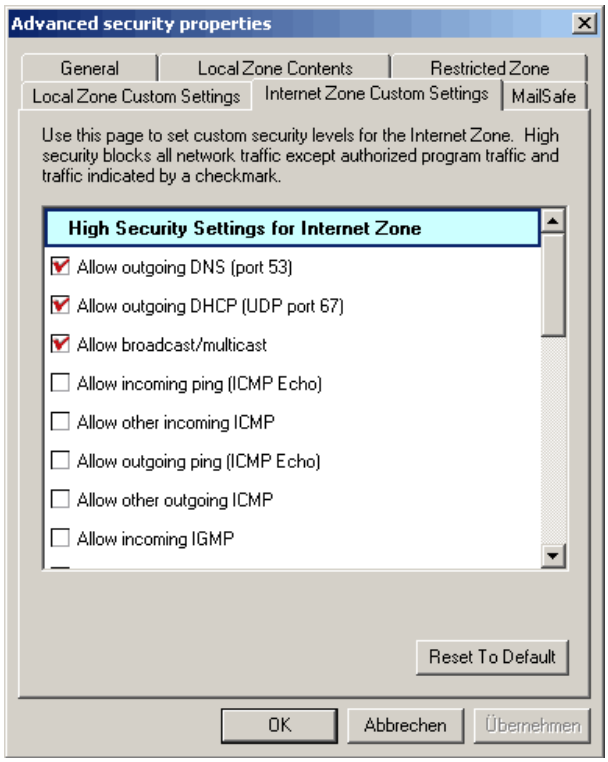
Zusätzlich kann man unter Ports noch jeder Anwendung gezielt die Zugriffe auf bestimmte Ports oder Server erlauben oder verbieten, und zwar getrennt nach Sicherheitszonen. So kann man z.B. zwischen Intranet und Internet unterscheiden und seinem Browser dort jeweils unterschiedliche Zugriffsrechte einräumen.



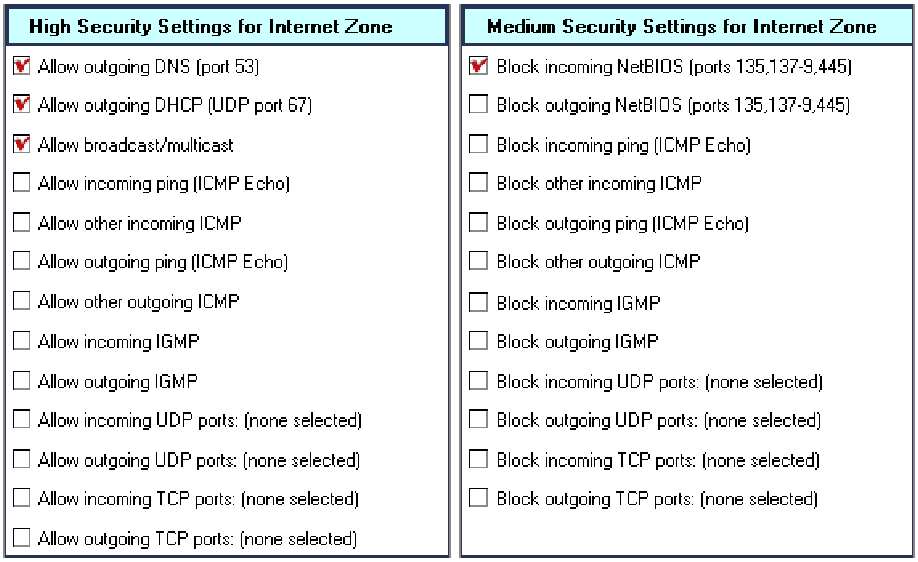
Genau wie zuvor ZoneAlarm unterscheidet nämlich auch ZoneAlarm Pro zwischen dem lokalem Netzwerk und dem Internet und durch die Schieberegler kann man wie wieder die Sicherheitsstufen für beide Zonen anpassen. Für das Internet sollte man auch hier nach Möglichkeit **High Security** wählen, um die eigenen Ports gegenüber anderen Internet-Teilnehmern zu verbergen.



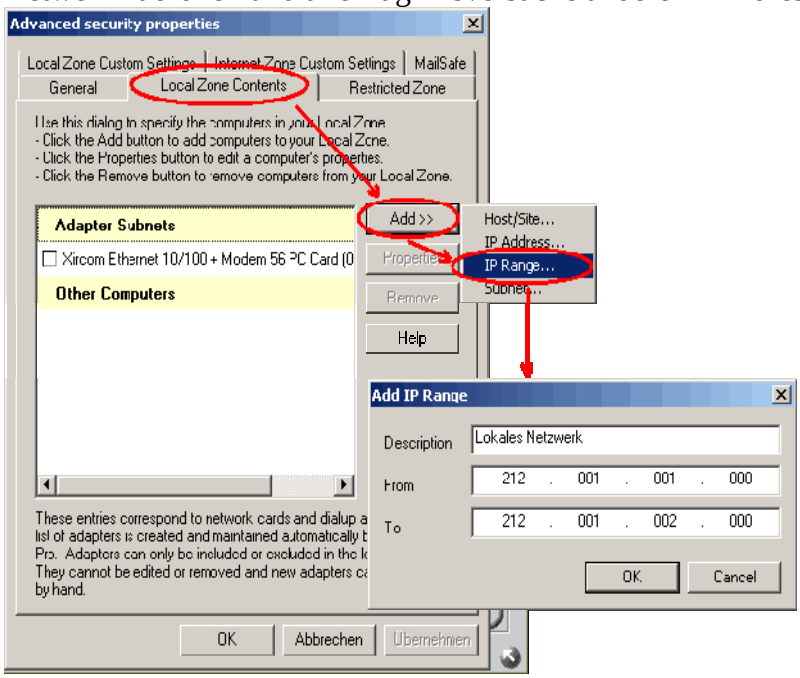
In ZoneAlarm Pro finden sich auch wesentlich mehr Einstellmöglichkeiten unter den **Security Settings**. Egal, welchen Schalter man hier drückt, es öffnet sich stets das gleiche Fenster. Lediglich der der entsprechende Menü-Eintrag ist schon entsprechend angewählt, wie z.B. hier das Menü für die Internet-Zone.



Hier kann man die vorgegebenen Sicherheitseinstellungen manuell seinen eigenen Wünschen anpassen.



Wer möchte kann die Sicherheitseinstellungen für jede der beiden Zonen nach Bedarf anpassen, um z.B. bestimmte Ports in eingehender oder ausgehender Richtung zu blockieren. Außerdem lassen sich den Zonen noch zusätzliche **Domänen**, **IP-Adressen** oder ganze **Subnets** zuordnen. So könnte man beispielsweise einen IP-Adressbereich dem lokalen Netwerk zuordnen und alle Zugriffsversuche anderer IP-Adressen komplett blockieren.



Wie man sieht, verdient ZoneAlarm Professional seinen Namen zu Recht. In Firmen kommt es beispielsweise häufig vor, dass ein Rechner gleichzeitig an ein lokales und ein fremdes Netzwerk (das muss nicht immer das Internet sein) angebunden ist. So kann man die Sicherheitseinstellungen für beide Zonen gezielt an seinen Wünschen anpassen und den Zugriff auf Ports, IP-Adressen, DNS-Services, Domänen etc. detailliert einstellen.
Wer jedoch kein eigenes Netzwerk hat und eigentlich nur ins Internet will, der findet die Unterteilung in zwei Zonen vielleicht etwas verwirrend. Eine andere Firewall, die für Surfer wirklich ideal ist, ist z.B. ATGuard.

Norton Internet Security

Diese Firewall basiert komplett auf ATGuard, welches von Symantec aufgekauft und nun als Norton Internet Security vermarktet wird. Unter der Norton-typischen Oberfläche verrichtet aber nach wie vor das originale ATGuard seine Dienste, wie man nach einem Blick hinter die Kulissen sehr schnell bemerken wird. Auch die Funktionen sind weitgehend identisch, so dass ich mir hier eine genauere Beschreibung erspare. Ich möchte hier lediglich auf die viel gestellte Frage eingehen, welches der beiden Programme nun das Empfehlenswertere ist, denn es liegt ja eigentlich nahe, dass ein neueres Produkt auch das Bessere ist. In diesem Fall stimmt das leider nicht ganz, denn technisch hat Symantec leider nicht viel Neues beigesteuert.

Die Neuerungen beschränken sich zur Zeit auf ein grafisches Menü, einer "Inhaltskontrolle" und etlichem überflüssigem Firlefanz wie z.B. dem Norton Live Update oder den Norton Web Services. Damit hat Symantec es geschafft, die ursprünglich 1.5 MB große Installationsdatei von ATGuard auf über 10 MB aufzublasen und das Norton Internet Security frisst dadurch unnötig viel Speicherplatz auf der Festplatte, sowie im laufenden Betrieb wesentlich mehr Ressourcen als nötig. Das praktische Dashboard wurde von Symantec ebenfalls entfernt.

Ein großes Sicherheitsproblem ist die automatische Regelerstellung von Norton Internet Security, die anhand einer Liste die gängigsten Applikationen über den Dateinamen erkennt und automatisch eine Regel dafür erstellt. Das ist auf den ersten Blick zwar bequem, erlaubt aber z.B. Trojanern, sich unter falschem Dateinamen unbemerkt Zugriff ins Internet zu verschaffen. Das ist natürlich nicht der Sinn einer Firewall und diese automatische Regelerstellung sollte man unbedingt deaktivieren, wenn man Wert auf ein geschütztes System legt.

Hinzu kommt, dass Symantec sich entschieden hat, NIS in drei verschiedene Produktlinien aufzuspalten und z.B. in der verkrüppelten Personal Edition den Werbe- und Cookieblocker entfernt hat. Wer sich also für das "neuere" Produkt entscheidet, sollte sich wenigstens vorher darüber informieren, welche der 3 erhältlichen Versionen für seine Zwecke ausreichend ist.

Personal Firewall
: Werbe- und Cookieblocker wurden entfernt

Internet Security
: Entspricht ungefähr ATGuard

Internet Security Family Edition
: Bietet zusätzlich noch eine Inhaltskontrolle

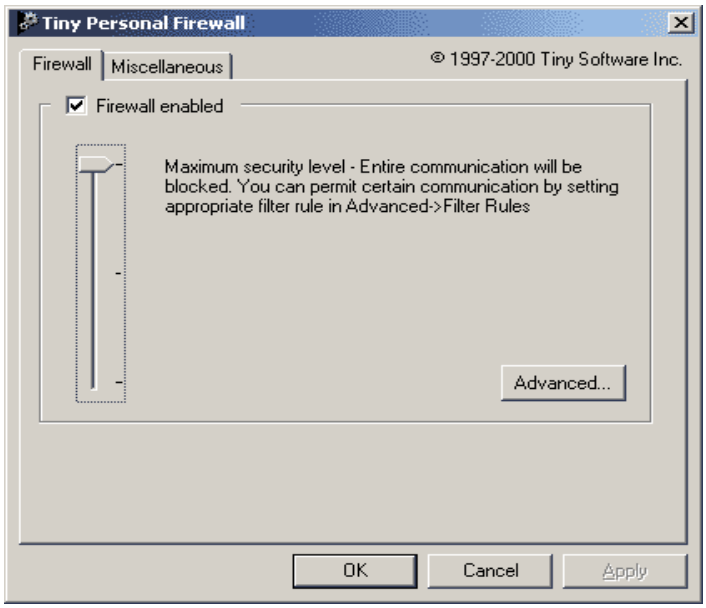
Man mag Symantec zugute halten, dass zumindest bei den letzten beiden Produkten noch der hauseigene Virenscanner **Norton Antivirus** mitgeliefert wird, aber dessen Systemperformance und Erkennungsroutinen, speziell im Bereich der Trojaner, können leider nicht mit Antiviral Toolkit Pro von Kaspersky Labs mithalten. Einen unbestreitbaren Vorteil bietet Norton Internet Security jedoch gegenüber ATGuard, nämlich die Verträglichkeit mit Windows ME.

Tiny Personal Firewall

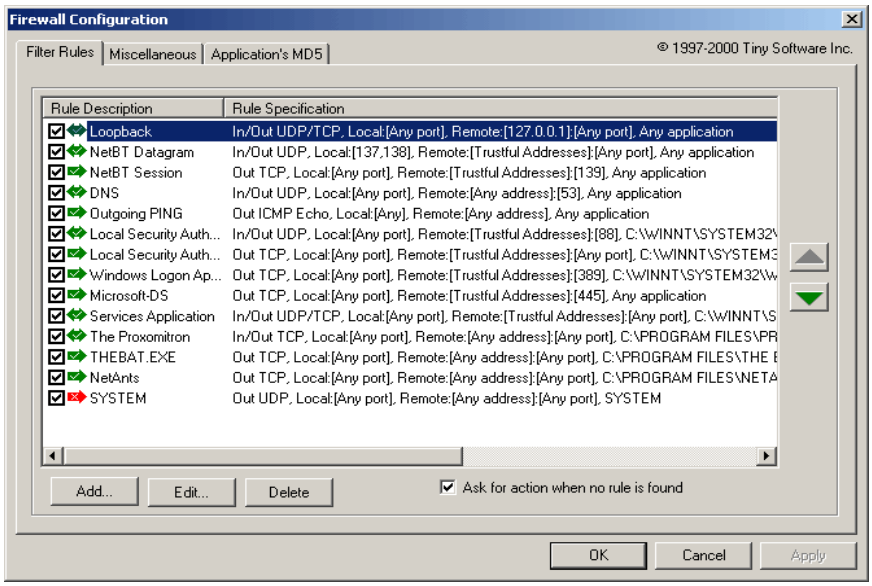
Ähnlich ZoneAlarm ist auch diese Firewall gratis erhältlich. Genau wie bei Zonealarm bedeutet es nicht, dass man ein schlechtes Produkt erhielte, wenn man nichts dafür bezahlen muss.

Ganz im Gegenteil: Tiny Personal Firewall stellt eine echte Alternative zu ATGuard dar, welches ja nicht mehr weiterentwickelt wird. Die im Vergleich zu ATGuard fehlenden Optionen wie z.B. Cookie- oder Werbefilter lassen sich mit anderen, gratis erhältlichen Programmen realisieren. Dazu aber später mehr...

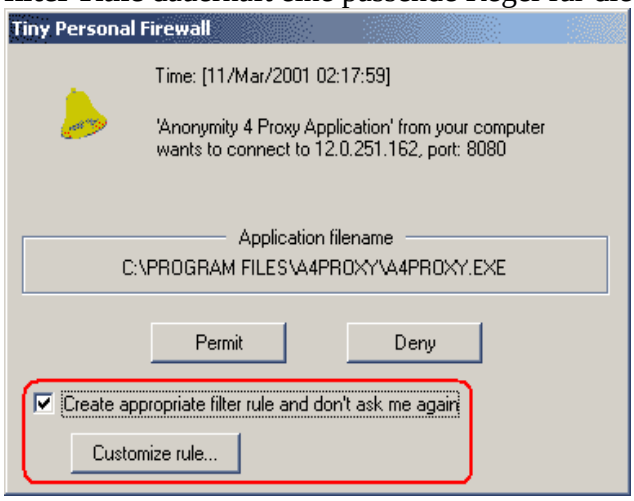
Nach der Installation der Tiny Personal Firewall bietet ein Schieberegler zunächst die Möglichkeit, vordefinierte Sicherheitslevel einzustellen. Es empfiehlt sich, hier die höchste Stufe einzustellen, bei der jegliche Kommunikation zunächst einmal verboten wird:



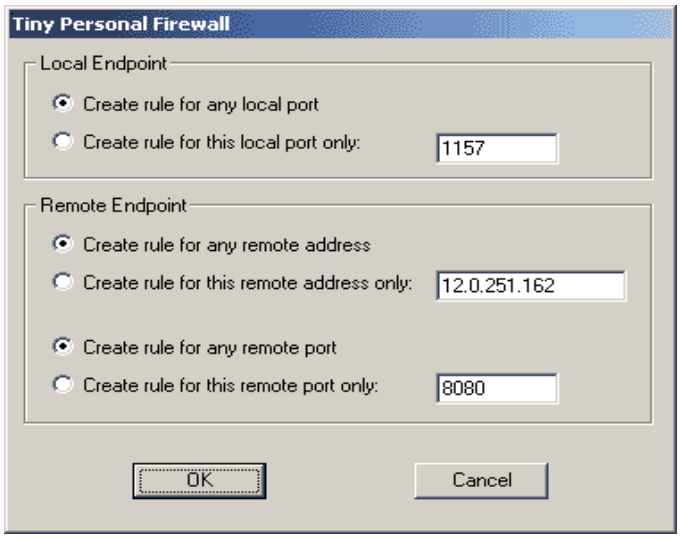
Nun sind zunächst zwar grundsätzlich keine Netzwerkverbindungen mehr möglich, was sich aber schnell beheben lässt, indem man einfach für jedes Programm, welches sich ins Internet verbinden darf, eine Regel aufstellt. Das Regelwerk dieser Firewall verbirgt sich hinter dem Knopf **Advanced**.



Die Regeln lassen sich entweder mit **Add** manuell hinzufügen, oder man benutzt einfach den Assistenten, den man mit der Option **Ask for action when no rule is found** anwählt. Zukünftig fragt Tiny Personal Firewall bei jeder unbekannten Anwendung nach, ob eine Verbindung erlaubt werden soll oder nicht. Man hat die Wahl, mit Permit und Deny den Zugriff nur für dieses eine Mal zu erlauben oder zu verbieten oder mit **Create appropriate filter Rule** dauerhaft eine passende Regel für die Zukunft zu erstellen:

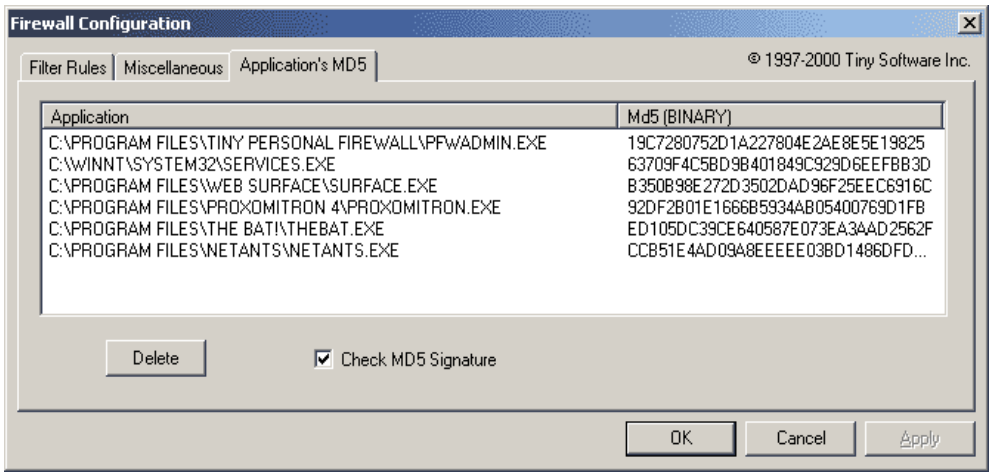


Eigentlich war das schon alles. Startet man nun ein neues Programm, meldet sich der Assistent zu Wort und fragt nach, ob man die Verbindung dieses Programmes erlauben oder verbieten möchte. Tiny Personal Firewall unterscheidet hier zwischen den Ports, durch die diese Verbindung stattfinden soll und der IP-Adresse, auf die der Zugriff erlaubt wird.



Beim Erstellen von Regeln gilt auch hier: Was nicht ausdrücklich durch das Erstellen einer Regel erlaubt wurde, ist verboten. Jedes Programm, das eine Verbindung herstellen möchte und nicht im Regelwerk der Firewall auftaucht, wird daran gehindert bzw. bei aktiviertem Assistenten fragt die Firewall nach, ob dafür eine neue Regel erstellt werden soll.

Tiny Personal Firewall identifiziert übrigens die Anwendungen nicht nur nach ihrem Dateinamen, sondern merkt sich außer dem Verzeichnispfad auch noch die MD5 Prüfsumme des entsprechenden Programmes. Ich möchte hier nicht weiter darauf eingehen, durch welche Algorithmen diese Prüfsumme generiert wird, weil ich das an dieser Stelle für unwichtig halte, sondern nur erwähnen, dass damit eine absolut sichere Identifizierung der Anwendungen ermöglicht wird. Durch diese Prüfsumme haben trojanische Pferde praktisch keine Chance, Programme unbemerkt zu infizieren oder sich unter deren Namen an Tiny Personal Firewall vorbeizuschleichen.



Die Generierung einer Prüfsumme ist ein nicht zu unterschätzender Vorteil gegenüber Firewalls, die Anwendungen lediglich anhand des Dateinamens erkennen können oder sogar, wie im Fall von Norton Internet Security, automatisch Programmen mit bestimmten Dateinamen per Voreinstellung den Zugriff erlauben.

Firewall installiert - nichts geht mehr

Wenn das Problem durch temporäres Deaktivieren der Firewall behoben ist, dann sollte man sich einmal die erstellten Regeln genauer betrachten. Offensichtlich verhindert eine davon die Verbindung ins Internet oder ins Netzwerk. Bringt die Änderung der entsprechenden Regel keinen Erfolg, so ist es am Einfachsten, sie zu löschen und den Regelassistenten, sofern vorhanden, zu aktivieren. Startet man dann das entsprechende Programm, so wird eine neue Regel für dieses Ereignis erstellt.

Mehrere Firewalls gleichzeitig nutzen?

In der Regel vertragen sich Firewalls gut miteinander. Lediglich die Tiny Personal Firewall scheint einige Probleme im Zusammenspiel mit anderen Produkten zu haben. Es spricht bei ausreichend vorhandenen Ressourcen des Rechners nichts dagegen, mehrere Produkte gleichzeitig zu benutzen, da jede Firewall ihre Stärken und Schwächen hat. Ein gutes Beispiel ist die Kombination von ATGuard ZoneAlarm, die sich recht gut ergänzen. Für den Normalgebrauch reicht aber eine gut konfigurierte Firewall sicher vollkommen aus. Mehr als zwei Firewalls benötigt man bestimmt nicht, man sollte es nicht übertreiben...

Firewall meldet Zugriffe von Außen

Es muss sich nicht immer um einen Angriff handeln, wenn irgendetwas aus dem Internet auf den eigenen Rechner zugreifen möchte. Meist handelt es sich dabei lediglich um einen **Ping**, d.h. ein Teilnehmer aus dem Internet möchte wissen, ob ihm eine bestimmte IP-Adresse antwortet. Die Gründe für solche Pings können unterschiedlicher Natur sein. Vielleicht sucht der entsprechende Teilnehmer gerade einen freien **FTP-Server** oder er hat andere Gründe, eine bestimmte IP-Adresse zu testen. Was es auch immer ist - niemanden braucht es zu interessieren, ob der eigene Rechner antwortet oder auch nicht. Genau so verhält es sich auch mit echten Trojaner-Angriffen, die man meist an den verwendeten Ports identifizieren kann, über die der fremde Rechner eine Verbindung herstellen will: Weg damit!

Ein unbekanntes Programm möchte ins Internet

In der Regel weiß man ja selbst, welche Programme man online benutzt. Browser, Mailprogramme, FTP-Programme oder ähnliche Anwendungen, die man ja meist schon am Namen identifizieren kann. Wenn darüber hinaus noch etwas Unbekanntes ins Internet möchte, so kann der Zugriff getrost verweigert werden. Was hat beispielsweise der Service **System** im Internet verloren? Genau: Nichts! Auch wenn das Wort System meinetwegen unglaublich wichtig klingen mag oder sogar Bestandteil des Betriebssystems ist, so hat das Ding keine Veranlassung, sich auf irgendwelche Server im Internet zu verbinden. Solange die eigenen, erwünschten Anwendungen noch funktionieren, dann kann's ja wohl nicht so wichtig gewesen sein. Stellt man dagegen nach dem Blockieren eines unbekannten Zugriffs fest, dass eine wichtige Anwendung nicht mehr funktioniert, so ist die entsprechende Regel normalerweise mit ein paar Mausklicks rasch wieder entfernt.

Wo bekommt man Rulesets für die Firewall her?

Es gibt eine Menge guter Rulesets für alle möglichen Firewalls. Interessant sind jedoch vor allem die Dokumentationen zum Verstehen, warum dieses oder jenes geblockt oder erlaubt wird. Das beste Ruleset erstellt man sich jedoch immer noch selbst, indem man dem Regel-Assistenten seiner frisch installierten Firewall zunächst alle auf dem eigenen Rechner vorhandenen Programme bekannt macht, die ins Internet dürfen und dann anschließend den Regel-Assistenten wieder abschaltet. Danach sollte ein kritischer Blick in die frisch installierten Regeln folgen, denn Manches lässt sich noch verbessern. Benötigt der Browser tatsächlich noch andere Ports außer dem Port 80? Sicher nicht. Und weshalb sollte man diesen Port, der sowieso nur vom Browser benutzt wird, für Zugriffe von Außen freigeben? Etwas Feintuning macht sich immer gut.