Benutzerhandbuch für Intego NetBarrier X5

Intego NetBarrier X5 für den Macintosh

Intego
www.intego.com

Inhaltsverzeichnis

1 – Über Intego NetBarrier X5

Was ist Intego NetBarrier X5?

Intego NetBarrier X5 ist die perfekte Internet-Sicherheitslösung für Macintosh-Computer, auf denen das Betriebssystem Mac OS X installiert ist. Dieses Softwareprodukt bietet einen umfassenden Schutz vor Versuchen, über das Internet oder ein lokales Netzwerk in Ihren Computer einzudringen.

NetBarrier X5 schützt Ihren Computer vor Eindringversuchen, indem alle über das Internet oder ein anderes Netzwerk ein- und alle ausgehenden Datenpakete kontinuierlich gefiltert werden. Mit NetBarrier X5 sind Sie vor Datendiebstahl, Hackerangriffen und Eindringversuchen geschützt. Die Software warnt Sie automatisch bei verdächtigen Aktivitäten.

NetBarrier X5 stellt vier separate Verteidigungslinien auf, um Ihren Mac vor Eindringversuchen und Angriffen zu schützen.

Persönliche Firewall

NetBarrier X5 enthält eine persönliche Firewall, die alle ein- und ausgehenden Datenpakete filtert. Standardmäßig stehen mehrere grundsätzliche Filterregeln zur Verfügung. Im Modus „Angepasst“ können Sie bei Bedarf zudem Ihre eigenen Regeln definieren.

Antivandalismus

Die Antivandalismus-Funktion von NetBarrier X5 ist ein leistungsstarker Schutz für Ihren Computer. Sie beobachtet die Netzwerkaktivitäten Ihres Mac und sucht nach Anzeichen für Eindringlinge. Wenn die Funktion eine verdächtige Aktivität entdeckt, stoppt NetBarrier X5 den Eindringling auf seinem Weg und zeigt einen Warnhinweis an. Die Funktion „Antivandalismus“ bietet zudem eine Sperrliste, in der die Adressen der Eindringlinge gespeichert werden, die versucht haben, in ihren Mac einzudringen. So werden diese Adressen immer blockiert. Intego NetBarrier X5 stellt Ihnen mehrere Optionen zur Verfügung, mit denen Sie die Software an Ihre individuellen Bedürfnisse anpassen können.

Richtlinie

NetBarrier X5 sperrt alle eingehenden Datenpakete, die als feindlich betrachtet werden. Intego NetBarrier X5 kann ein Dialogfeld mit einer Warnmeldung öffnen, woraus hervorgeht, weshalb die Datenpakete gesperrt wurden. Gleichzeitig werden Sie aufgefordert, den Empfang der Datenpakete zu erlauben oder abzulehnen. Sie können auch andere Alarmoptionen wählen. Beispielsweise können Sie festlegen, dass ein akustischer Alarm ausgegeben werden soll, dass die Internet-Adresse des sendenden Computers automatisch in die Sperrliste aufgenommen werden soll oder dass an die von Ihnen angegebenen E-Mail-Adressen eine E-Mail gesendet werden soll.

Sperrliste

Wenn entdeckt wird, dass ein Eindringling versucht in Ihren Mac einzudringen, bietet NetBarrier X5 Ihnen die Möglichkeit, diesen auf eine Sperrliste zu setzen, in der die Netzwerkadresse gespeichert wird. Wenn ein Computer mit der gleichen Adresse versucht, noch einmal in Ihren Computer einzudringen, wird er automatisch blockiert.

Vertrauenswürdige Gruppe

In manchen Fällen sperrt NetBarrier X5 auch Verbindungen mit Computern Ihrer Bekannten. Hierbei kann es sich um Computer in Ihrem lokalen Netzwerk handeln, die beispielsweise nur deshalb gesperrt werden, weil sie Ihren Computer „anpingen“. Mit NetBarrier X5 können Sie die Internet-Adressen dieser „befreundeten“ Computer als Computer einer vertrauenswürdigen Gruppe deklarieren. So werden diese Computer solange als „befreundet“ betrachtet, wie Sie möchten - und können stets auf Ihren Computer zugreifen. Beachten Sie auf jeden Fall, dass die Vertrauenswürdige Gruppe nur für die Antivandalismus-Funktion und die Datenfilter von NetBarrier X5 gilt und dass die Firewall-Regeln weiterhin auf die Computer in der Vertrauenswürdigen Gruppe angewendet werden.

Anti-Spyware

NetBarrier X5 ermöglicht es Ihnen, festzulegen, welche Programme aufs Internet und/oder auf Ihr lokales Netzwerk zugreifen dürfen. Wenn ein nicht vertrauenswürdiges Programm versucht, auf ein Netzwerk zuzugreifen, kann NetBarrier X5 eine Warnmeldung ausgeben, um Sie darüber zu informieren, welches Anwendungsprogramm versucht, die Verbindung herzustellen. Wenn Sie dem betreffenden Anwendungsprogramm den Zugriff erlauben wollen (wenn es wirklich ein Programm ist, von dem Sie wissen, dass es das Netzwerk

verwenden sollte), können Sie dies tun. Wenn ein Programm aber eine Netzwerkverbindung heimlich herstellen will, können Sie ihm auf Dauer den Netzwerkzugriff verwehren.

Schutz persönlicher Daten

NetBarrier X5 bietet Ihnen einen Schutz Ihrer persönlichen Daten. Das Programm filtert die Daten und stellt so sicher, dass keine sensiblen Informationen Ihren Computer verlassen. Es blockiert zudem Werbebanner und lässt Sie anonym surfen. Ferner können Sie mit Intego NetBarrier X5 folgende Informationen über Ihren Computer verbergen: das Betriebssystem, den verwendeten Webbrowser und die zuletzt von Ihnen aufgerufene HTML-Seite.

Überwachung

NetBarrier X5 beinhaltet leistungsstarke Funktionen, mit denen Sie Ihre Netzwerkaktivitäten und die Verwendung des Netzwerkes überwachen können. Anzeigepegel geben das Netzwerk-Datenverkehrsaufkommen in Echtzeit wieder. Ferner werden Informationen über Ihren Computer, das lokale Netzwerk sowie aktive Dienste und Verbindungen angezeigt.

NetBarrier X5 bietet sogar ein separates Programm, NetBarrier Monitor, das Sie immer geöffnet lassen können sowie einen Überwachungsbildschirmschoner. So behalten Sie Ihren Netzwerkdatenverkehr immer im Blick.

So löschen Sie Ihre Spuren mit Washing Machine

NetBarrier X5 beinhaltet ein separates Programm namens Washing Machine, das Ihre Privatsphäre noch mehr schützt: Es unterstützt Sie dabei, Informationen über Ihre Internetgewohnheiten zu löschen. Es bietet eine einfache Möglichkeit, Lesezeichen, Cookies, Caches, Verläufe geladener Dateien und Browserverläufe aus mehr als zwei Dutzend Programmen zu entfernen, die diese Informationen regelmäßig speichern. Das Programm kann auch so eingestellt werden, dass es diese Elemente regelmäßig löscht. So erhalten Sie einen mühelosen Schutz.

Washing Machine beinhaltet Funktionen, die in früheren Versionen von NetBarrier enthalten waren. Sie können das Programm aus dem Intego-Menü im Untermenü NetBarrier X5 starten. Weitere Informationen über die Verwendung von Washing Machine finden Sie im Benutzerhandbuch von Washing Machine, das Sie mit NetBarrier X5 erhalten haben.

So verwenden Sie dieses Benutzerhandbuch

Wenn Sie:	**Lesen Sie:**
Eine Privatperson mit Internet-Zugang sind	• Kapitel 2, **Einführung in die Datensicherheit** • Kapitel 3, **Installation** • Kapitel 4, **Erste Schritte** • Optional: Kapitel 5 - 8, **Die vier Verteidigungslinien**. NetBarrier X5 ist so konfiguriert, dass Ihr Computer automatisch vor Eindringlingen geschützt wird.
Ein Mitarbeiter eines Unternehmens oder einer anderen Organisation mit Anschluss an ein lokales Netzwerk und das Internet sind	• Kapitel 2, **Einführung in die Datensicherheit** • Kapitel 3, **Installation** • Kapitel 4, **Erste Schritte** Die grundlegenden Schutzmodi von NetBarrier X5 werden Ihnen vermutlich ausreichen. Eventuell sollten Sie jedoch auch die Kapitel 5 - 8, **Die vier Verteidigungslinien** lesen.
Ein Benutzer, der seinen Computer als Server betreibt oder ein Netzwerk verwaltet sind	Sie sollten das ganze Benutzerhandbuch durchlesen. Von besonders großer Bedeutung für Sie dürften die Kapitel 5 - 8, **Die vier Verteidigungslinien** sein, insbesondere Kapitel 5, in dem erklärt wird, wie Sie Ihre eigene Regeln definieren können.

Am Ende dieses Handbuchs finden Sie Glossar mit häufig verwendeten Fachbegriffen.

2 – Einführung in die Datensicherheit

Weshalb Ihr Computer unbedingt vor Angriffen geschützt werden sollte

Unabhängig davon, ob Sie Ihren Mac zum Arbeiten oder nur zum Surfen im Internet verwenden, ob Sie den ganzen Tag über oder nur ab und zu online sind, ob Ihr Computer isoliert oder mit einem lokalen Netzwerk verbunden ist, ob Sie Privatperson oder Mitarbeiter eines Unternehmens oder einer anderen Organisation sind: Ihr Computer enthält sensible und damit schützenswerte Informationen. Bei diesen Informationen kann es sich um Ihre Kreditkartennummer, Ihre Bankkontodaten, Verträge mit Kunden oder Mitarbeitern, Dokumente zu vertraulichen Projekten oder um E-Mail-Mitteilungen oder Passwörter handeln. Ganz egal, welche vertraulichen Informationen Sie auf Ihrem Mac gespeichert haben: irgendwo da draußen in den Weiten des Internet gibt es bestimmt jemanden, der sich dafür interessieren könnte.

Je intensiver Sie Ihren Mac für Ihre tägliche Arbeit oder Ihr Hobby nutzen, umso mehr sollten Sie die darauf befindlichen Informationen schützen.

Vergleichen Sie einfach Ihren Computer mit einem Haus! Bevor Sie Ihr Haus verlassen, werden Sie höchstwahrscheinlich alle Fenster schließen und alle Türen absperren. Aber schützen Sie Ihren Mac auf die gleiche Weise? So lang Ihr Computer mit einem Netzwerk verbunden ist, haben raffinierte Hacker und Kriminelle die Möglichkeit, auf die Daten zuzugreifen, die auf Ihrem Computer gespeichert sind. Dagegen können Sie sich aber optimal mit NetBarrier X5 schützen.

Wenn Ihr Mac mit einem Netzwerk verbunden ist - ganz gleich, ob Sie ihn nur privat nutzen, er in ein Netzwerk integriert ist, oder er mit dem Internet verbunden ist: er ähnelt prinzipiell einen Haus an einer Straße mit Türen und Fenstern. NetBarrier X5 funktioniert wie eine Reihe von Schlössern und schützt auf diese Weise Ihre Türen und Fenster. Wenn Sie eine HTML-Seite aufgerufen haben, wissen Sie niemals, wer dies beobachten kann. Wenn Sie beispielsweise auf eine Website mit Informationen über Computerspiele gehen und dort nach Tricks suchen, wie Sie Ihre Gegner überlisten können, lauert dort vielleicht ein Hacker auf Sie, der Ihren Mac ausspionieren will, um zu sehen, ob er etwas interessantes finden kann. Ein anderer denkbarer Fall wäre, dass Sie eine Website mit Aktienkursinformationen besuchen, die von einem neugierigen Hacker überwacht wird, der nun versucht, die Computersysteme der Websitebesucher „nur zum Spaß“ zu beschädigen.

Ohne Intego NetBarrier X5 werden Sie vielleicht nie erfahren,
ob irgendjemand versucht, auf Ihren Mac zuzugreifen.

Ein Computer ist nur so sicher wie die Leute, die Zugriff darauf haben. NetBarrier X5 schützt Ihren Mac, indem der Zugriff vom Netzwerk durch Unbefugte sowie das Versenden sensibler Informationen gesperrt wird.

Wie kann ein Computer vollkommen sicher gemacht werden?

Es gilt als allgemein bekannt, dass ein Computer nur sicher gemacht werden kann, indem man ihn ausschaltet, alle Verbindungen mit ihm abtrennt, ihn in einem mit Titan verstärkten Safe verschließt, diesen in einem atombombensicheren Bunker einmauert, die äußeren Räume mit Giftgas erfüllt und vor dem Bunker hoch bezahlte, bewaffnete Wachen postiert. Da dies nun einmal sehr unpraktisch ist, muss eine andere Lösung gesucht werden. Schließlich wollen Sie in der Lage sein, mit Ihrem Computer zu arbeiten.

Die optimale Lösung dieses Problems ist NetBarrier X5. Diese Software bietet Ihnen Schutz, der weit über das hinausgeht, was die meisten Computer-Benutzer benötigen. Durch seine auf einfachste Weise an jede Situation anpassbaren Firewall-Regeln ist Intego NetBarrier X5 das perfekte Hilfsmittel für System- und Netzwerkverwalter, die damit in der Lage sind, dem Schutze an Ihre spezifischen Anforderungen anzupassen.

Was ist eine Firewall?

Eine Firewall (deutsche Übersetzung: Brandschutzmauer) funktioniert wie eine Wand. Sie schützt Ihren Computer oder Ihr lokales Netzwerk, indem Benutzer in zwei Gruppen untergliedert werden: diejenigen innerhalb der Wand und die anderen außerhalb. Eine Firewall wird so konfiguriert, dass Personen außerhalb der Firewall nur unter bestimmten Bedingungen Zugriff auf die Computer innerhalb der Firewall haben können. Das Gleiche gilt auch umgekehrt.

Eine Firewall ist eine Art Filter zwischen Ihrem Computer oder LAN (Local Area Network = lokales Netzwerk) und einem WAN (Wide Area Network = Weitverkehrsnetz) wie dem Internet. Die Firewall filtert Datenpakete und prüft, woher sie kommen und wohin sie gehen.

NetBarrier X5 bietet einen leistungsstarken Firewall-Schutz für Ihren Mac. Der maßgeschneiderte Schutz bietet erfahrenen Benutzern die Möglichkeit, bestimmte Regeln zu konfigurieren, um den Computer vor Gegnern zu schützen, die dort eindringen möchten.

Freund oder Feind?

Damit jemand durch eine Wand gehen kann, muss diese eine Tür enthalten. Die Funktion „Antivandalismus“ von NetBarrier X5 fungiert als Filter oder Wachpersonal, das die Tür einer Wand bewacht und alle ein- und ausgehenden Daten auf Anzeichen von Hackern, Vandalen, Spionen, Eindringlingen und Dieben prüft. Dies ist möglich, da in ein ungeschütztes Computersystem auf mehrere unterschiedliche Weisen eingedrungen werden kann, und NetBarrier X5 diese Verfahren erkennt.

Was Sie riskieren

Weshalb Leute in Computersysteme eindringen

Dafür, dass manche Leute in fremde Computersysteme einzudringen versuchen, gibt es mehrere Gründe. Manchmal versuchen Hacker, von fremden Computern aus in andere Computersysteme einzudringen, um ihre Spuren zu verwischen. Dies ist möglich, indem Verbindungen zwischen so vielen Computersystemen wie möglich hergestellt werden, sodass der Computer, von dem aus der Hacker operiert, nicht identifiziert werden kann.

Andere Leute versuchen, in fremde Computersysteme einzudringen, weil ihnen dies Spaß macht und sie immer neue Möglichkeiten dazu herausfinden müssen. Dies ist so ähnlich wie mit den Graffitisprayern, die ihre „Kunstwerke“ oftmals nur in die Welt setzen wollen, damit diese wahrgenommen werden.

Allerdings gibt es auch richtige Kriminelle, die versuchen, in Computer anderer Leute einzudringen. Hierbei kann es sich um Wirtschaftsspione handeln, die Informationen über Aktivitäten, Projekte und Kunden eines Konkurrenzunternehmens ausspähen wollen. Oder um Diebe, die Passwörter und Kreditkartennummern ausspionieren, um sich geldwerte Vorteile zu verschaffen. Die meisten Unternehmen haben Richtlinien zur Datensicherheit ausgearbeitet, doch nur wenige Unternehmen kümmern sich um die Sicherheit ihrer Unternehmensdaten auf den Privatcomputern ihrer Mitarbeiter. Viele Angestellte arbeiten auch zuhause für ihr Unternehmen, sodass auch die Privatcomputer von Mitarbeitern geschützt werden müssten.

Unglücklicherweise leben wir in einer Welt, in der sich fast alles zu Geld machen lässt. Da die heutige Wirtschaft vor allem auf Informationen basiert, ist es kein Wunder, dass es heutzutage lukrativer ist, Informationen als Edelmetalle zu stehlen. Hier ist ein einfaches Beispiel: Am Muttertag im vergangenen Jahr haben Sie Ihrer Mutter Blumen gekauft. Diese hatten Sie per Fax bestellt, da Sie Ihre Kreditkartennummer nicht übers Internet versenden wollten. Da Sie das Fax von Ihrem Computer aus versandt haben, ist das gefaxte Dokument mit der Kreditkartennummer immer noch auf der Festplatte Ihres Computers gespeichert. Wenn nun jemand beispielsweise übers Internet in Ihr Computersystem eindringt, kann er dieses Dokument auf seinen Computer kopieren und mit Ihren Kreditkartenangaben Einkäufe zu Ihren Lasten tätigen.

Die unterschiedlichen Arten möglicher Angriffe und Eindringversuche

Es gibt viele Gründe, aus denen Leute versuchen, in die Computersysteme anderer einzudringen. Und es gibt vermutlich ebenso viele Verfahren, um dies zu tun. Einige Gründe sind folgende:

- Das „Stehlen“ vertraulicher Dokumente und Informationen.
- Das Ausführen von Befehlen auf Ihrem Computer, um das Betriebssystem zu verändern, Ihre Festplatte zu löschen oder Ihren Computer auf sonstige Weise zu beschädigen.
- Das Verfremden von Websites durch Ersetzen von Seiten durch anderen Text und/oder andere Grafiken.
- Das Durchführen von DoS-Angriffen (DoS, Denial of Service = Dienstverweigerung) mit dem Ziel, einen fremden Computer so mit Datenpaketen zu überschwemmen, dass er auf keine anderen Anfragen mehr reagieren kann.
- Das Erfassen von Informationen über Ihren Computer, um einen späteren Versuch eines Eindringens in Ihr Netzwerk oder Ihren Computer zu starten.

Schutz persönlicher Daten

Sie werden vermutlich nicht wissen, wie viele Informationen über Sie von Websites abgefragt werden, wenn Sie ganz normal im Internet surfen. Beim Besuch mancher Websites werden Sie gebeten, sich anzumelden. Hier müssen Sie einen Benutzernamen und ein Passwort eingeben. Gelegentlich werden Sie auch aufgefordert, Ihren Namen, Ihre Postadresse und andere Informationen einzugeben. Diese Informationen werden häufig dazu verwendet, Ihr Surfverhalten und Ihre Interessen zu analysieren, um Ihnen speziell auf Ihre Wünsche zugeschnittene Produkte und Dienstleistungen anzubieten.

Immer mehr Internet-Benutzer weigern sich, den Betreibern von Websites persönliche Informationen zur Verfügung zu stellen. Manchmal gibt es hierfür auch einen wirklich triftigen Grund: Sie melden sich beispielsweise bei einer Website an, und später erhalten Sie unaufgefordert eine Vielzahl von Werbemitteilungen per E-Mail. Wenn dies geschieht, ist es allerdings meistens zu spät.

Website-Server können aber auch noch andere Informationen über Sie und Ihr Verhalten abfragen. Wussten Sie, dass Ihr Webbrowser bei jedem Besuch einer Website Informationen darüber versendet, welches Betriebssystem und welchen Webbrowser Sie verwenden, und sogar, welche HTML-Seite Sie als letzte aufgerufen haben?

Ein weiteres Problem stellen so genannte Cookies dar. Hierbei handelt es sich um eine kleine Datei, die ein Website-Server auf der Festplatte Ihres Computers speichert. Beim nächsten Besuch der gleichen Website wird das Cookie von Ihrem Webbrowser an eben diesen Website-Server zurückgesandt. Typischerweise werden Cookies dazu verwendet, um einen Benutzer wieder zu erkennen, nachdem er sich einmal bei einer Website angemeldet hat. Dadurch müssen die Anmeldeinformationen wie Benutzername und Passwort nicht mehr eingegeben werden. Cookies werden auch dazu verwendet, um einen „Einkaufskorb“ mit Waren zu verwalten, die Sie auf einer Seite zum Kauf ausgewählt haben. Oder um eine Seite zu personalisieren (unterschiedlichen Personen werden verschiedene Seiten angezeigt). Oder um den Zugriff eines bestimmten Benutzers auf eine Seite zu überwachen.

Cookies haben durchaus ihre Berechtigung, können aber auch zum Analysieren Ihres Surfverhaltens verwendet werden. Diese Daten werden dann unter Umständen an Unternehmen verkauft, die Ihnen nun Produkte und Dienstleistungen anbieten, die zu Ihrem individuellen Surfverhalten passen. Es kommt sogar vor, dass die Banner, die Sie beim Besuch von Websites zu sehen bekommen, auf Grund dieser gesammelten Informationen über Ihr Surfverhalten aktiviert werden.

NetBarrier X5 bietet Ihnen auf einfachste Weise einen Schutz Ihrer persönlichen Daten: Sie können festlegen, dass bestimmte Arten von Informationen über Sie nicht von Ihrem Computer gesendet werden können.

3 – Installation

Systemanforderungen

- Jeder offiziell unterstützte Mac OS X-kompatible Computer
- Mac OS X 10.4 oder höher, Mac OS X Server 10.4 oder höher
- 40 MB freier Festplattenspeicherplatz

Installieren von Intego NetBarrier X5

Informationen über die Installation und Registrierung von NetBarrier X5 finden Sie im Handbuch für die ersten Schritte von Intego, das Ihrer Kopie von NetBarrier X5 beiliegt. Wenn Sie Intego NetBarrier X5 gekauft haben, indem Sie das Programm von der Intego-Website heruntergeladen haben, befindet sich dieses Handbuch in der Disk Image-Datei mit der Software, die Sie heruntergeladen haben. Wenn Sie NetBarrier X5 auf einer CD oder DVD gekauft haben, finden Sie dieses Handbuch auf der CD/DVD.

4 – Erste Schritte

So verwenden Sie Intego NetBarrier X5

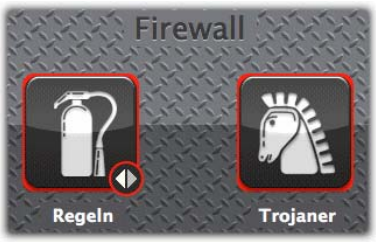
Wenn Sie NetBarrier X5 das erste Mal öffnen, wird Ihnen das Hauptfenster angezeigt. Wenn Sie eine ältere Version von NetBarrier verwendet haben, werden Sie feststellen, dass dieses Fenster vereinfacht und modernisiert wurde. Aber keine Sorge: alle alten Funktionen sind noch da.

So verwenden Sie das Hauptfenster von NetBarrier X5

Über das Hauptfenster erhalten Sie einen schnellen Zugriff auf:

- Die Funktionen, Einstellungen und Protokolle von NetBarrier X5
- mehrere hilfreiche Netzwerkdienstprogramme, wie Whois und Traceroute.
- grafische Anzeigen dafür, welche Schutzarten aktiviert sind,
- Informationen über das Programm selbst, z.B. wann es zuletzt aktualisiert wurde,
- eine Möglichkeit mehrere Konfigurationen zu verwalten, damit Sie die Schutzeinstellungen schnell ändern können.

In der Mitte des Hauptfensters gibt es Bereiche, mit denen Sie die vier Verteidigungslinien von NetBarrier X5 steuern können. Bedienungselemente für die Firewall-, Antivandalismus- und Datenschutzfunktion erscheinen als große Schaltflächen in der Mitte des Hauptfensters. Die Bedienungselemente für die Überwachung sind die kleineren Schaltflächen in der unteren rechten Ecke.

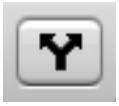


Im Abschnitt für die Firewall können Sie auf die Regeln zugreifen, die festlegen, welche Programme Informationen von Ihrem Mac senden und welche Programme Informationen auf Ihrem Mac empfangen dürfen. Sie erhalten ebenfalls Zugriff auf die Einstellungen für Trojanische Pferde, mit denen Sie Ihren Mac vor schädlichen Trojanischen Pferden schützen können.

Im Datenschutzbereich können Sie auf die Einstellungen zugreifen, die dafür sorgen, dass bestimmte Daten nicht über das Internet und lokale Netzwerke versendet werden und die bestimmte Arten von Informationen sperren, die während Sie im Internet surfen gesendet und empfangen werden.

Im Abschnitt Antivandalismus können Sie Ihre Richtlinien zum Sperren bestimmter Angriffsarten ansehen und steuern. Sie können einstellen, wie Sie vor bestimmten Programmen geschützt werden, die sich heimlich mit Remote-Computern verbinden (Anti-Spyware) und Sie können Ihre Sperrliste ansehen und bearbeiten, die die schlimmen Typen im Auge behält. Zudem können Sie auch die vertrauenswürdige Gruppe von Freunden ansehen und bearbeiten, denen der Zugriff auf Ihren Mac ausdrücklich erlaubt wird.

Über die Schaltflächen in der unteren rechten Ecke des Hauptfensters können Sie auf die Überwachungsfunktionen zugreifen. Sie können auf diese Funktionen auch über die Auswahl im Menü „Ansicht“ oder mithilfe von Tastenkombinationen zugreifen. Dabei handelt es sich um Folgende:

	**Protokoll**	Wahltaste-Befehlstaste-L	Zeigt eine Aufzeichnung der Aktivitäten von NetBarrier und des Datenverkehrs an, der von Ihrem Mac ins Internet oder in lokale Netzwerke abgeht oder von dort empfangen wird.
	**Verkehr**	Wahltaste-Befehlstaste-1	Zeigt den ein- und ausgehenden Netzwerkverkehr auf Ihrem Mac an.
	**Dienste**	Wahltaste-Befehlstaste-2	Zeit eine Liste von Wegen an, auf denen Ihr Mac Informationen an die Außenwelt liefern kann.
	**Netzwerke**	Wahltaste-Befehlstaste-3	Zeigt Außen-Netzwerke an, die derzeit für Ihren Mac zur Verfügung stehen.
	**Whois**	Wahltaste-Befehlstaste-4	Zeigt Informationen über die Eigentümer und Verwalter von Internetdomänen an.
	**Traceroute**	Wahltaste-Befehlstaste-5	Zeigt den Netzwerkpfad an, den ein Signal nimmt, um von Ihrem Mac zu einem anderen Computer zu gelangen.

Jede dieser Funktionen wird in Kapitel 8, **Die vier Verteidigungslinien: Überwachung** beschrieben.

Links im Hauptfenster finden Sie eine Konfigurationsliste. Jede Konfiguration ist eine Sammlung von Einstellungen für den Firewall-, Daten- und Antivandalismusschutz von NetBarrier. Zunächst gibt es nur eine Konfiguration namens „Standard“. Das runde Optionsfeld zeigt an, welche Konfiguration gerade aktiv ist.

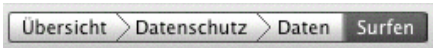
Am unteren Rand der Konfigurationsliste befinden sich vier Schaltflächen, mit denen Sie die Konfigurationen duplizieren, bearbeiten, entfernen und verbergen können. (Sie können auch zwischen dem Ein- und Ausblenden der Konfigurationsliste hin- und herwechseln, indem Sie Befehlstaste-K drücken oder „Ansicht > Konfigurationsliste ein-/ausblenden“ wählen.) Weitere Informationen finden Sie im Kapitel 10, **Einstellungen und Konfigurationen**.

Ganz oben im Hauptfenster befindet sich die NetUpdate-Statusleiste. Sie zeigt die Daten der neuesten NetBarrier-Filter an, die auf Ihrem Mac installiert sind, sowie die Daten der neuesten Filter, die über Intego NetUpdate erhältlich sind. NetUpdate sucht regelmäßig nach Aktualisierungen. Sie können das Programm auch sofort nach Aktualisierungen suchen lassen, indem Sie auf die Schaltfläche „Jetzt prüfen...“ in der oberen rechten Ecke klicken. Wenn Sie die Statusleiste von NetUpdate ausblenden möchten, wählen Sie „Ansicht > Statusleiste für NetUpdate ausblenden“. Weitere Informationen finden Sie im Benutzerhandbuch von NetUpdate.

Schließlich gibt es eine kleine Schaltfläche in der Nähe der oberen linken Ecke des Hauptfenster, die anzeigt, welchen Abschnitt der NetBarrier X5-Oberfläche Sie gerade ansehen. Wenn Sie das Programm das erste Mal öffnen, zeigt die Schaltfläche einfach „Übersicht“ an.

Wenn Sie jedoch auf den Kontrollbildschirm für Trojanische Pferde sehen, sehen Sie beispielsweise eine Schaltfläche, die deutlich anzeigt, dass sie zum Abschnitt „Firewall“ gehört, zusammen mit den Regeln.

Wenn Sie auf „Regeln“ klicken, gelangen Sie zu den Regeln. Wenn Sie auf „Firewall“ oder „Übersicht“ klicken, gelangen Sie zurück zum Hauptfenster. Die Abschnitte für Datenschutz und Antivandalismus funktionieren auf die gleiche Weise.



Statusanzeigen im Hauptfenster

Der Status vieler NetBarrier X5-Funktionen wird als Teil der Symbole im Hauptfenster angezeigt. Wenn die Abschnitte für Trojanische Pferde, Daten und Anti-Spyware aktiviert sind, sehen Sie ein kleines Kontrollhäkchen in der unteren rechten Ecke des jeweiligen Symbols.

	
Aus	Ein

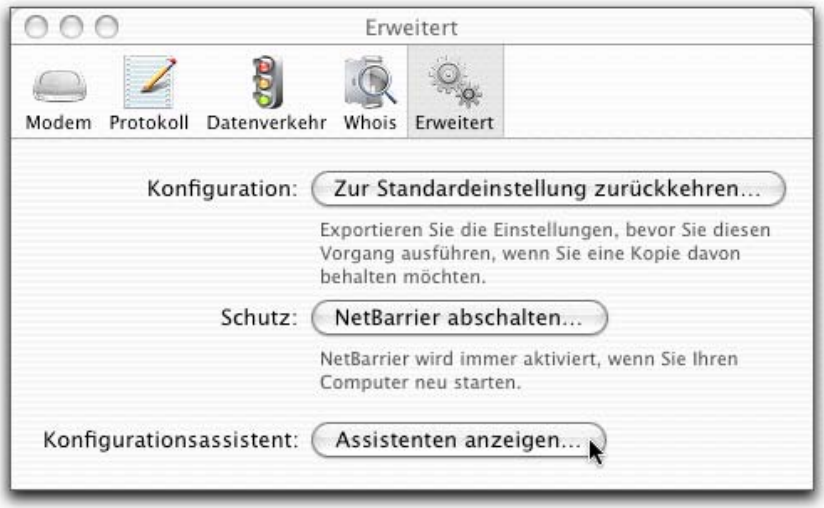
In ähnlicher Weise zeigen die Symbole für die Sperrliste und für die vertrauenswürdige Gruppe an, wie viele Einträge in der Liste sind.

	
Kein	Zwei

So verwenden Sie den Konfigurationsassistenten

Wenn Sie Ihren Macintosh nach der Installation von NetBarrier X5 neu starten, beginnt die Software automatisch damit, Ihren Macintosh zu schützen. Die Firewall wird im Client-, lokalen Servermodus aktiviert. Zudem werden alle Aktivitäten im Protokoll aufgezeichnet. In diesem Modus kann Ihr Mac als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen. Weitere Informationen über die Firewall-Modi von NetBarrier X5 erhalten Sie weiter vorn in diesem Handbuch.

NetBarrier X5 enthält einen Konfigurationsassistenten, mit dem Sie die Basiskonfiguration der Software schnell und einfach durchführen können. So passen Sie die Einstellungen an Ihre Art des Netzwerkeinsatzes an. Wenn Sie NetBarrier X5 zum ersten Mal öffnen, wird der Konfigurationsassistent automatisch gestartet. Wenn Sie von einer vorherigen Version von NetBarrier aktualisieren, müssen Sie den Konfigurationsassistenten manuell starten. Wählen Sie hierzu „NetBarrier X5 > Einstellungen“ und klicken Sie dann auf das Symbol „Erweitert“. Klicken Sie anschließend auf „Assistenten anzeigen…“ am unteren Fensterrand. Um den Konfigurationsassistenten ausführen zu können, benötigen Sie ein Administratorkennwort.



Klicken Sie auf den nach rechts weisenden Pfeil, um mit der Konfiguration von NetBarrier X5 zu beginnen. Indem Sie auf den nach links weisenden Pfeil klicken, können Sie jederzeit zu vorherigen Schritten zurückkehren; es öffnet sich dann das entsprechende Fenster. Der Konfigurationsassisten von NetBarrier X5 zeigt kurz einige Infofenster über die verschiedenen Funktionen des Programms an:

- **Firewall (Regeln und Trojanische Pferde)**
- **Datenschutz (Daten- und Surfschutz)**
- **Antivandalismus (Richtlinien, Anti-Spyware, Sperrliste und vertrauenswürdige Gruppe)**
- **Überwachung (das Protokoll und fünf Überwachungsfunktionen)**
- **Noch eine weitere Sache (verschiedene Funktionen)**

Wenn Sie fertig sind, können Sie im Konfigurationsfenster auswählen, welche Konfiguration von NetBarrier X5 Sie verwenden möchten.

Dabei handelt es sich um folgende Konfigurationen:

Name	**Am besten wenn...**	**Firewall-Einstellung**	**Andere Einstellungen**
Standard	...Sie einen Zugriff auf Ihren Mac von einem lokalen Netzwerk zulassen müssen, aber vor Eindringversuchen von außerhalb Ihres lokalen Netzwerks geschützt sein möchten.	Modus „Client, lokaler Server“: Ihr Mac kann als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen.	Alle Antivandalismus- und Datenschutzfilter sind deaktiviert.
Normal	...Sie Ihren Computer nicht als Netzwerkserver oder für das lokale Filesharing verwenden.	Modus „Nur Client“: Ihr Mac funktioniert nur als Client in einem lokalen Netzwerk oder im Internet. Die Server-	Antivandalismusfilter sind gegen Pufferüberlauf-Angriffe, Eindringversuche, Ping-Angriffe, Port-Scans und SYN-Flooding aktiviert.

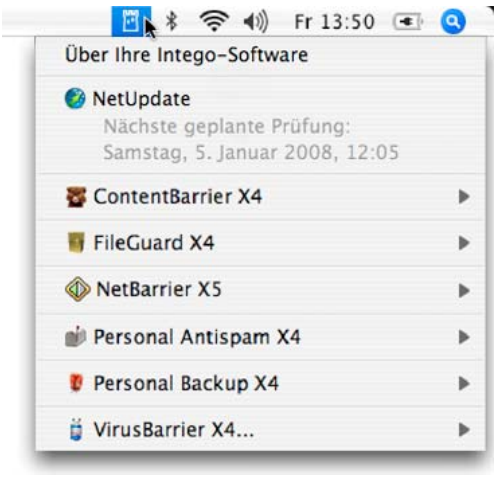
		Funktionen Ihres Computers sind gesperrt.	Für Ping-Übertragungen sind sie hingegen deaktiviert.
Stark	...Sie maximalen Schutz wünschen und akzeptieren können, dass diese Konfigurationen einigen Datenverkehr sperren kann.	Modus „Nur Client“.	Alle Antivandalismus-Filter sind deaktiviert, wie beispielsweise die, die vor Trojanischen Pferde schützen.

Klicken Sie zur Aktivierung der von Ihnen ausgewählten Konfiguration auf die Schaltfläche „Konfigurieren“.

So verwenden Sie das Intego-Menü

Mit NetBarrier X5 wird genau wie mit allen anderen Intego-Programmen ein so genanntes Intego-Menü in der Menüleiste installiert. Das Symbol dieses Menüs ist der kleine Turm aus dem Intego-Logo.

Wenn Sie auf das Intego-Menü klicken, wird Ihnen ein Menü mit der gesamten, auf Ihrem Computer installierten Intego-Software angezeigt:



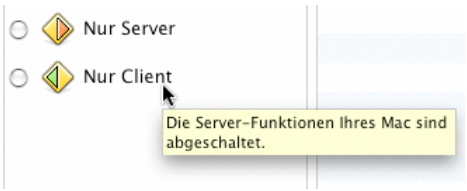
Aus dem Intego-Menü können Sie viele Einstellungen von NetBarrier X5 ändern. Wählen Sie das „Intego-Menü > NetBarrier X5“. Sie können Konfigurationen ändern und Sie können Einstellungen ein- und ausschalten, wie beispielsweise die Filterung oder Einstellungen für den Datenschutz. Sie können Intego Washing Machine aus dem Intego-Menü öffnen, indem Sie das Intego-Menü wählen und dann „NetBarrier X5 > Washing Machine öffnen...“. Und Sie können NetBarrier Monitor öffnen, indem Sie „NetBarrier X5 > NetBarrier Monitor öffnen“ wählen.

Passwortschutz von NetBarrier X5

NetBarrier X5 verwendet den in Mac OS X integrierten Passwortschutz. Sie können das Programm nur installieren und konfigurieren, wenn Sie Administratorprivilegien haben und sich mit einer entsprechenden Benutzerkennung und einem Passwort bei Ihrem Computer anmelden. Benutzer, die nicht über Administratorprivilegien verfügen, können die Einstellungen von NetBarrier X5 nicht verändern. Diese Benutzer können zwar die Monitor-Funktionen ansehen, wie beispielsweise Protokolle und Anzeigepegel, aber Sie dürfen keine Änderungen an den Programmfunktionen vornehmen.

So rufen Sie die Hilfe auf

Sie erhalten Hilfe für einige Funktionen von NetBarrier X5, indem Sie den Mauszeiger über den entsprechenden Bereich ziehen:



Eine QuickInfo zeigt Ihnen dann eine Erklärung der entsprechenden Funktion an.

Eine vollständige Hilfe erhalten Sie, indem Sie dieses Handbuch aufrufen. Wählen Sie hierzu „Hilfe > Benutzerhandbuch für NetBarrier X5“.

5 – Die vier Verteidigungslinien: Firewall

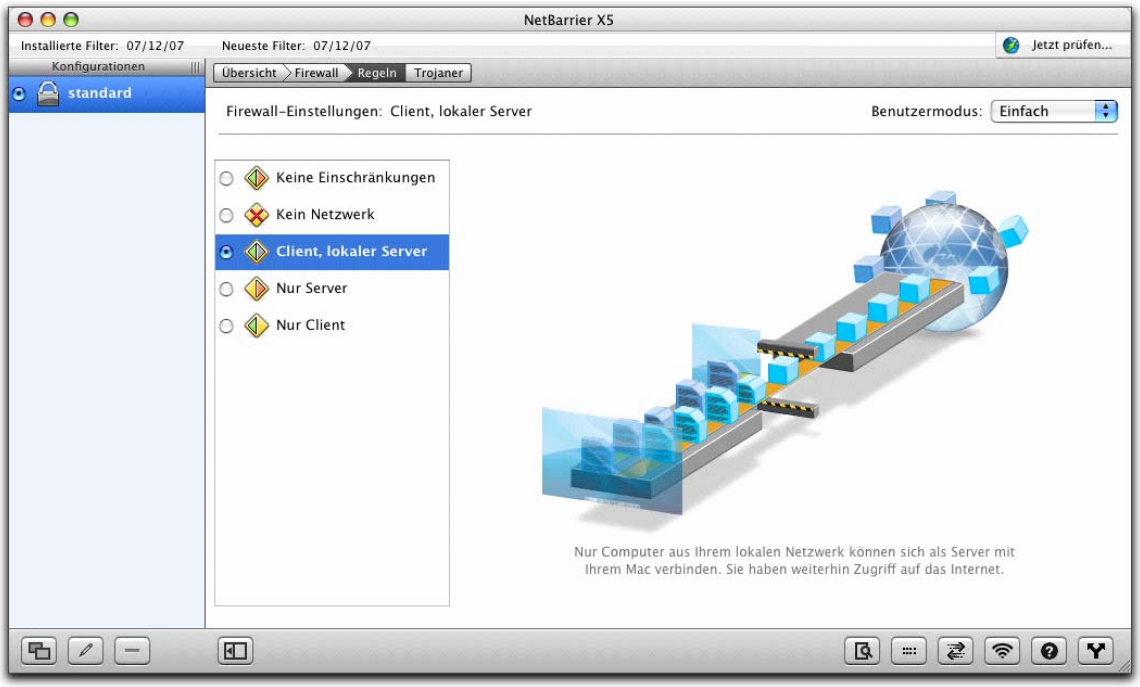
NetBarrier X5 ist ein leistungsfähiges und einfach anzuwendendes Programm, das Ihren Mac durch vier Verteidigungslinien während der Verbindung mit einem Netzwerk schützt. Die erste dieser vier Verteidigungslinien ist eine persönliche Firewall. Dabei handelt es sich um ein leistungsstarkes Programm, das alle Datenpakete filtert, die bei Ihrem Mac über das Internet oder ein lokales TCP/IP-Netzwerk ein- und ausgehen. Die Firewall schützt auch vor Trojanischen Pferden, indem die von diesen verwendeten Ports gesperrt werden.

Im Hauptfenster wird der Abschnitt „Firewall“ angezeigt, der zwei Schaltflächen enthält: Regeln und Trojaner.

Firewall-Regeln

Einfacher Modus

Wenn Sie auf die Schaltfläche „Regeln“ klicken, zeigt NetBarrier X5 den einfachen Modus zur Steuerung der Firewall-Einstellungen an. Es gibt fünf voreingestellte Firewall-Konfigurationen, die alle Situationen abdecken, die bei normaler Verwendung eintreten können. Jede Einstellung wird von einer Animation begleitet, die die Auswirkungen bei Anwendung der Einstellung grafisch anzeigen. Das Fenster direkt vor Ihnen repräsentiert Ihren Mac. Der Globus steht für das Internet und das Fenster zwischen den beiden repräsentiert die Grenzen Ihres lokalen Netzwerks. Die Standardeinstellung hier, „Client, lokaler Server“, zeigt an, wie Ihr Computer Informationen von außerhalb des lokalen Netzwerks empfangen kann, aber die Computer außerhalb Ihres lokalen Netzwerks können nicht auf Ihren Mac zugreifen.



Die folgende Abbildung zeigt die fünf Firewall-Einstellungen und wie Sie im Hauptfenster angezeigt werden:

Keine Einschränkungen 	Die Firewall von NetBarrier X5 erlaubt das Senden und Empfangen aller ein- und ausgehenden Netzwerkdaten.
Kein Netzwerk 	Die Firewall von NetBarrier X5 sperrt den Empfang und den Versand sämtlicher Daten aus einem und in ein lokales TCP/IP-Netzwerk bzw. aus dem/ins Internet. Dieser Modus ermöglicht es Ihnen, jeden Netzwerk-Datenverkehr Ihres Computers zu sperren, wenn Sie beispielsweise von Ihrem Computer abwesend sind.
Client, lokaler Server 	Die Firewall von NetBarrier X5 erlaubt die Verwendung Ihres Mac als Client und als lokaler Netzwerkserver. Ihr Mac kann als Client-Computer auf das Internet zugreifen und Ihr Mac kann sowohl als Client als auch als Server in einem lokalen Netzwerk dienen.
Nur Server 	Die Firewall von NetBarrier X5 erlaubt nur die Verwendung Ihres Mac als Server: Alle Client-Funktionen, einschließlich der Fähigkeit im Internet zu surfen, sind blockiert.

Nur Client 	Die Firewall von NetBarrier X5 erlaubt nur die Verwendung Ihres Mac als Client in einem lokalen Netzwerk oder im Internet. Die Server- und Filesharing-Funktionen Ihres Mac sind gesperrt.

Diese fünf Einstellungen sind für die meisten Leute ausreichend. Wenn Sie jedoch mehr Kontrolle über den Zugriff auf Ihren Computer möchten, wenn Sie beispielsweise eine Spieleparty durchführen und den gesamten Datenverkehr verbieten möchten, außer der Kommunikation zwischen den Spielteilnehmern, müssen Sie in den erweiterten Modus von NetBarrier X5 wechseln.

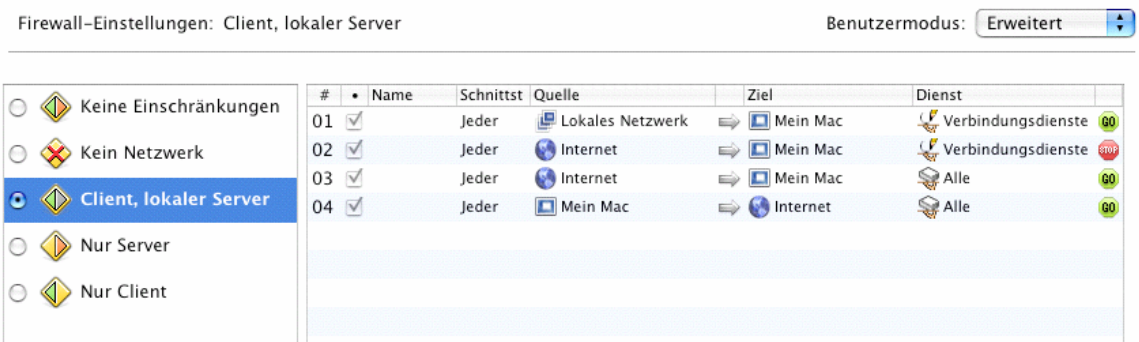
Erweiterter Modus

Jede der zuvor beschriebenen fünf Einstellungen ist in Wirklichkeit eine Sammlung von Regeln, von denen jede durch das Benennen von erlaubten und verbotenen Quellen, Zielen, Diensten und Schnittstellen definiert wird. Im einfachen Modus dürfen Sie die Regeln oder Teile davon nicht verändern. Hierzu müssen Sie in den erweiterten Modus im Firewall-Fenster wechseln.

Ändern Sie den Benutzermodus im Popup-Menü in der oberen rechten Ecke von „Einfach“ in „Erweitert“, um auf den vollständigen Satz von Firewall-Regeln in NetBarrier X5 zugreifen zu können.

ACHTUNG: Das Ändern dieser Einstellungen kann schwerwiegende Auswirkungen auf die Fähigkeit Ihres Computers haben, auf lokale Netzwerke und das Internet zuzugreifen. Sie sollten den erweiterten Modus nur verwenden, wenn Sie die Auswirkungen und die Funktionsweise wirklich verstehen.

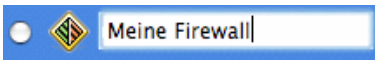
Im einfachen Modus wird eine Animation angezeigt, wenn Sie auf die fünf voreingestellten Firewall-Konfigurationen klicken. Im erweiterten Modus werden Ihnen die Einzelheiten der Regeln für jede einzelne Einstellung angezeigt.



In diesem Beispiel hat die Einstellung „Client, lokaler Server“ vier Regeln. Die erste erlaubt dem lokalen Netzwerk den Zugriff auf Ihren Mac über alle verbundenen Dienste. Das sind TCP-Verbindungen, die mit einer Kommunikation in beide Richtungen verbunden sind, wie beispielsweise das zur Verfügung stellen von Dateien von Ihrem Mac. Die zweite Regel jedoch verbietet solche Verbindungen über das Internet und lässt Ihren Mac somit nicht als Server für einen unbekannten Computer außerhalb Ihres lokalen Netzwerks dienen. Die dritte Regel erlaubt alle anderen Kommunikationsarten aus dem Internet mit Ihrem Mac und die vierte erlaubt alle Kommunikationsarten von Ihrem Mac *zum* Internet.

Die fünf voreingestellten Firewall-Einstellungen werden „eingefroren“, damit Sie praktisch und stabil sind: Sie können die Regeln oder die Reihenfolge, in der sie erscheinen, nicht ändern. NetBarrier X5 bietet Ihnen zwei Möglichkeiten, um zusätzliche, eigene Einstellungen zu erstellen: über den Assistenten und manuell.

In jedem Fall müssen Sie zuerst auf die Schaltfläche „+“ unter der Liste mit den Einstellungen klicken. Daraufhin wird eine neue Einstellung namens „unbenannte Einstellungen“ angezeigt. Klicken Sie darauf und geben Sie einen beliebigen Namen ein. Drücken Sie dann auf die Eingabetaste, um die Änderung dauerhaft zu akzeptieren.



Denken Sie bitte daran, dass Sie die Einstellung jetzt nur erstellt haben, Sie haben sie aber noch **nicht** aktiviert. Am besten aktivieren Sie die Firewall-Einstellungen erst, wenn Sie alle Ihre Regeln hinzugefügt haben. Klicken Sie zum Aktivieren der Einstellung auf das runde Optionsfeld links neben der entsprechenden Einstellung.

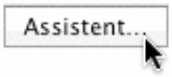
So erstellen Sie Regeln mit dem Assistenten

NetBarrier X5 enthält einen Assistenten, der Sie dabei unterstützt, Ihre eigenen Firewall-Regeln zu definieren. Dank diesem Assistenten werden hierfür nur wenige Mausklicks benötigt. Mit dem Regelassistenten können Sie zwar nicht auf alle Regeln von NetBarrier X5 zugreifen, doch decken die damit definierbaren Regeln die meisten Anwendungsfälle ab. Wenn Sie eine weitergehende Anpassung an Ihre Anforderungen wünschen, können Sie die Regeln zunächst mit dem Regelassistenten definieren und anschließend manuell modifizieren.

Der Regelassistent von NetBarrier X5 führt Sie durch mehrere Schritte zur Definition einer Regel:

- **Name und Verhalten**
- **Richtung**
- **Dienst**
- **Optionen**
- **Beenden**

Wenn Sie eine neue Regel definieren wollen, müssen Sie auf die Schaltfläche „Assistent“ klicken.



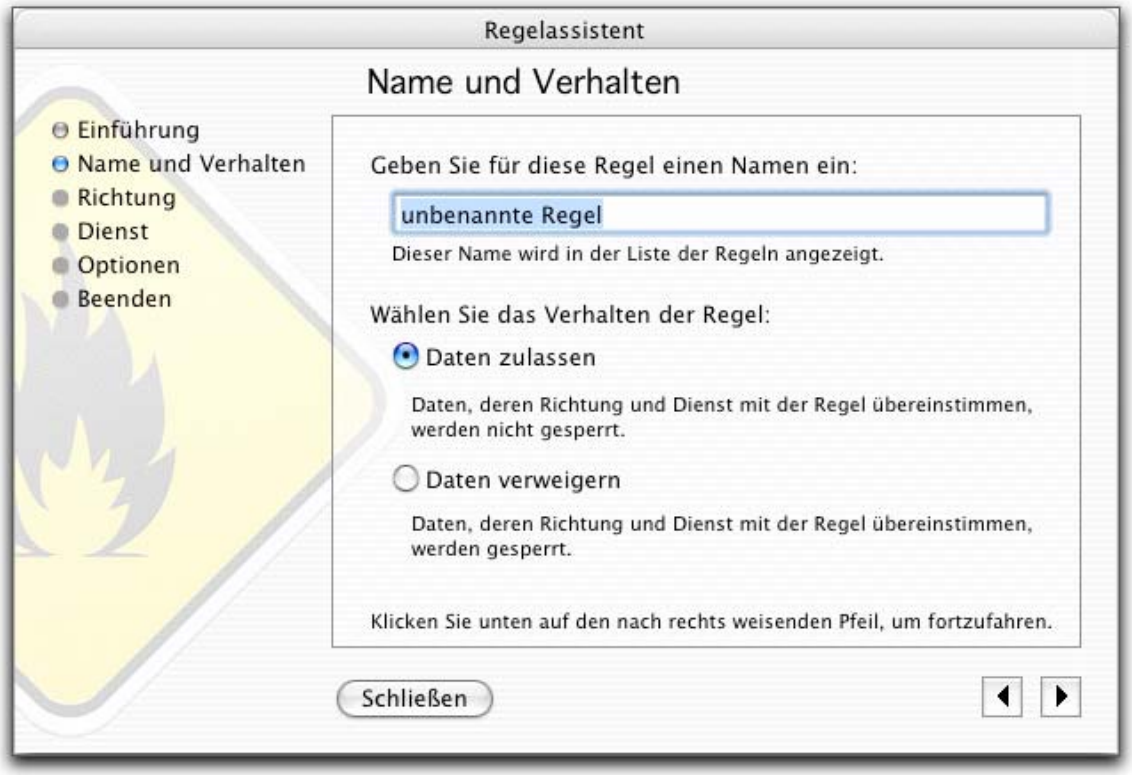
Hierauf wird das erste Dialogfeld des Regelassistenten geöffnet.

Klicken Sie auf den nach rechts weisenden Pfeil, um mit dem Definieren der Regel zu beginnen. Indem Sie auf den nach links weisenden Pfeil klicken, können Sie jederzeit zu vorherigen Schritten zurückkehren; es öffnet sich dann das entsprechende Fenster.

Alternativ können Sie auf „Schließen“ klicken, um den Regelassistenten zu beenden.

Name und Verhalten

In diesem Dialogfeld können Sie Ihrer neuen Regel einen Namen geben.

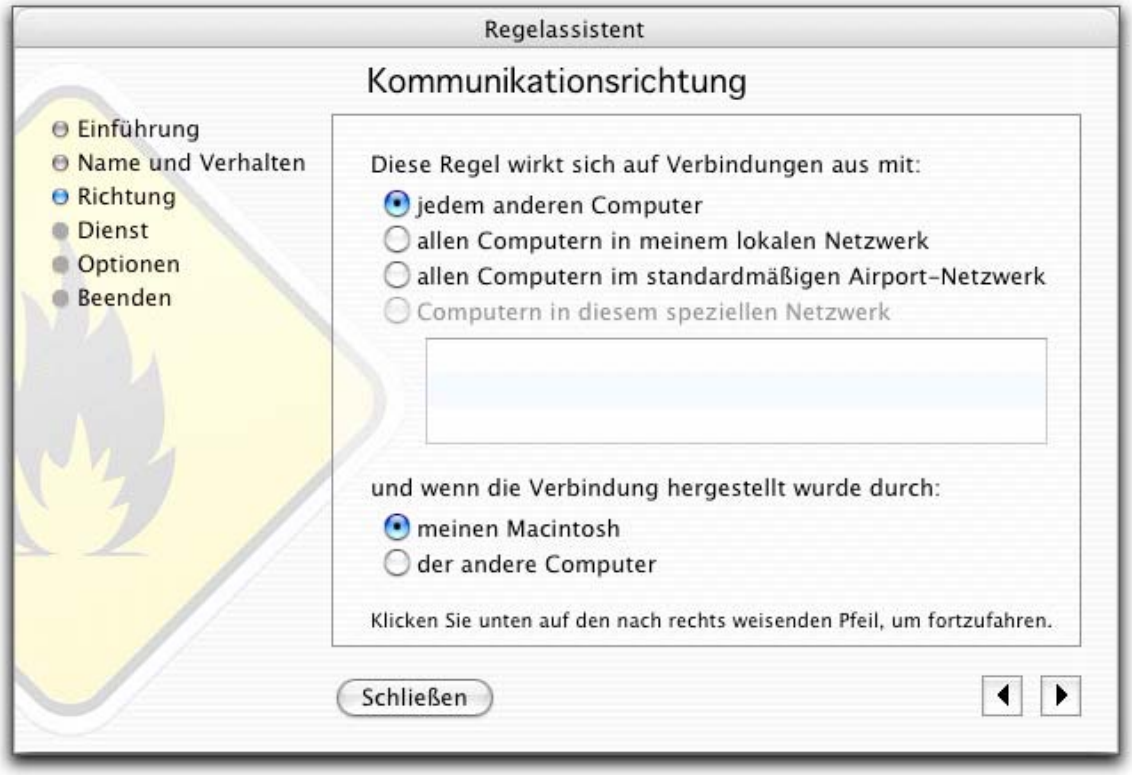


Geben Sie einen Namen ins entsprechende Feld ein und wählen Sie das Verhalten der neuen Regel: „Daten erlauben“ oder „Daten ablehnen“. Wenn Sie die Option „Daten erlauben“ gewählt haben, gibt die Regel die Daten gemäß Transportrichtung und Dienst frei. Wenn Sie die Option „Daten ablehnen“ gewählt haben, sperrt die Regel die Daten gemäß Transportrichtung und Dienst.

Klicken Sie auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Kommunikationsrichtung

In diesem Dialogfeld können Sie die Richtung des Datentransfers und den Computer wählen, von dem die Verbindung hergestellt wird.



Wählen Sie zuerst im Abschnitt **Diese Regel wirkt sich auf Verbindungen aus mit:** einen entfernten Server aus. Für die Auswahl des entfernten Servers bestehen vier Möglichkeiten:

Jedem anderen Computer	Hierbei handelt es sich um jeden anderen Computer, der nicht Ihr Macintosh ist.
Computern in meinem lokalen Netzwerk	Hierbei handelt es sich um jeden anderen Computer im gleichen Netzwerk, mit dem auch Ihr Macintosh verbunden ist.
Computern im standardmäßigen Airport-Netzwerk	Hierbei handelt es sich um jeden Computer, der mit Ihrem standardmäßigen AirPort-Netzwerk (sofern vorhanden) verbunden ist.

Computern in diesem speziellen Netzwerk	Wenn Sie mit dem Regelassistenten ein spezielles Netzwerk definiert haben, können Sie dieses Netzwerk wählen.

Wählen Sie nun den Computer, von dem die Verbindung hergestellt wird:

Mein Macintosh	Hierbei handelt es sich um Ihren Macintosh, also den Computer, der diese Regel anwendet.
Der andere Computer	Hierbei handelt es sich um den entfernten Server, den Sie im ersten Abschnitt dieses Dialogfelds definiert haben.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Dienst

In diesem Dialogfeld können Sie den Dienst wählen, auf den sich die Regel auswirkt.

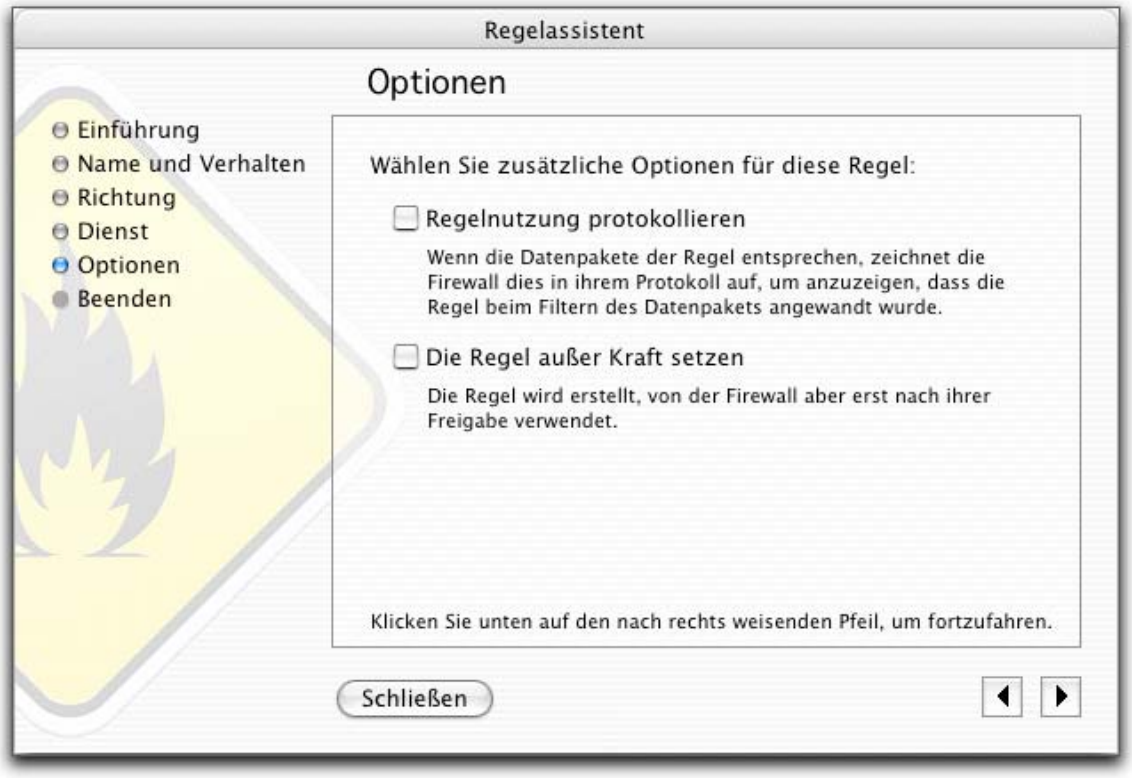
Drei Arten von Diensten stehen Ihnen zur Auswahl:

Alle Dienste	Alle Netzwerk-Dienste.
TCP-Dienste (Verbindungsdienste)	Dienste, die eine bestehende Verbindung zwischen zwei Computern erfordern, also die Dienste HTTP, FTP, TELNET, SSH, POP3, AppleShare, usw. Dies betrifft alle TCP-Verbindungen.
Dieser Dienst	Sie haben die Auswahl aus mehreren Diensten für populäre Anwendungsprogramme und Internet-Datenübertragungsprotokolle. Klicken Sie auf den Namen des gewünschten Dienstes in der Liste.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Optionen

In diesem Fenster können Sie zusätzliche Optionen für Ihre neue Regel wählen.



In diesem Dialogfeld werden zwei Optionen zur Auswahl angeboten:

Regelnutzung protokollieren	Die Firewall speichert jedes Mal, wenn diese Regel angewendet wurde, im Protokoll.
Die Regel außer Kraft setzen	NetBarrier X5 erstellt die Regel zwar, deaktiviert sie jedoch. Sie können die inaktive Regel später aktivieren.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

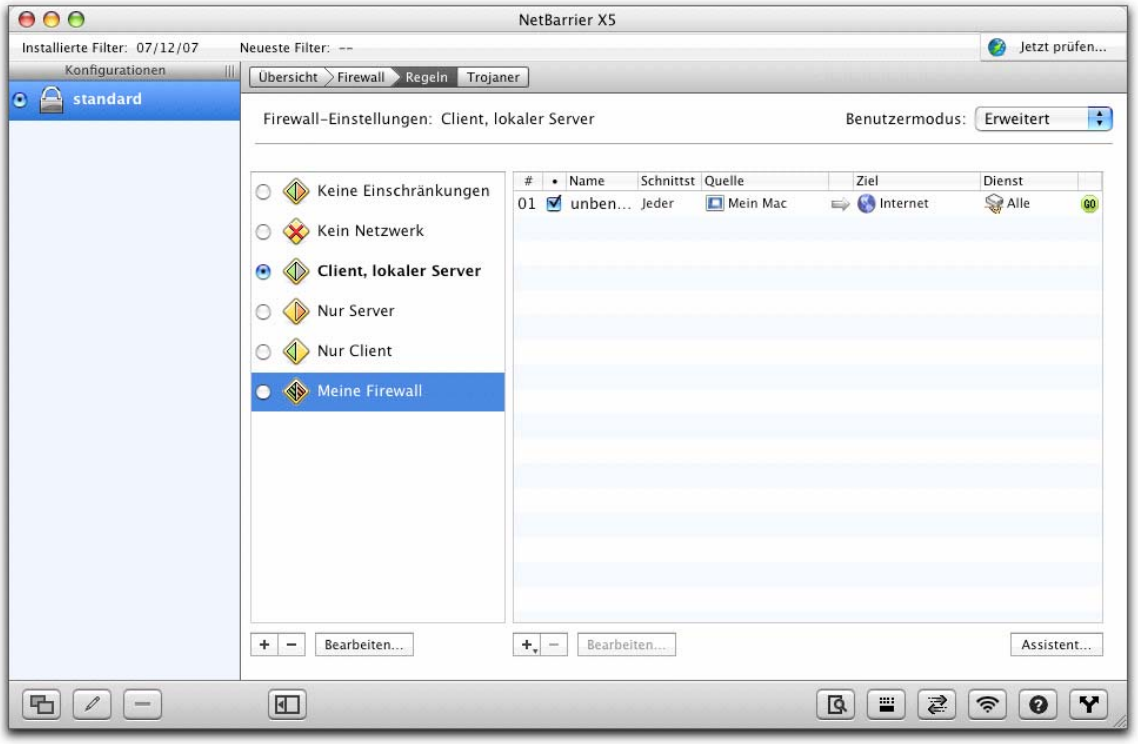
Beenden

In diesem Dialogfeld wird das Erstellen der Regel gemäß den mit dem Regelassistenten vorgenommenen Einstellungen bestätigt.

In diesem Dialogfeld wird nur eine einzige Option zur Auswahl angeboten: Wenn Sie das Kontrollkästchen **Regel für die Datenübertragung in Gegenrichtung erstellen** markieren, erstellt der Regelassistent eine übereinstimmende Regel mit Vertauschung von Datenquelle und Datenziel.

Klicken Sie auf die Schaltfläche „Erstellen“, um eine neue Regel zu definieren und den Regelassistenten zu beenden.

Nach dem Erstellen der Regel werden Sie sehen, dass die Regel bzw. Regeln (wenn Sie das Kontrollkästchen **Regel für die Datenübertragung in Gegenrichtung erstellen** markiert haben) in der Liste der Firewall-Regeln angezeigt wird bzw. werden.

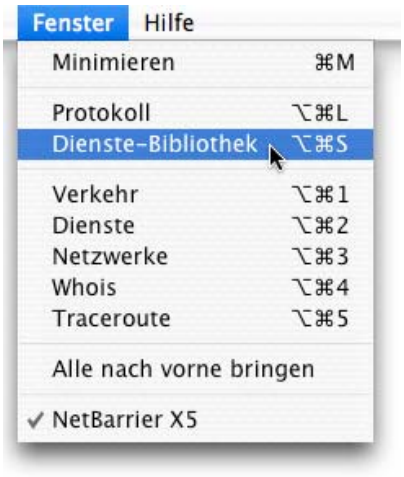


Wenn Sie die Regel modifizieren wollen, gehen Sie bitte gemäß dem Unterabschnitt „Ändern von Regeln“ weiter unten vor.

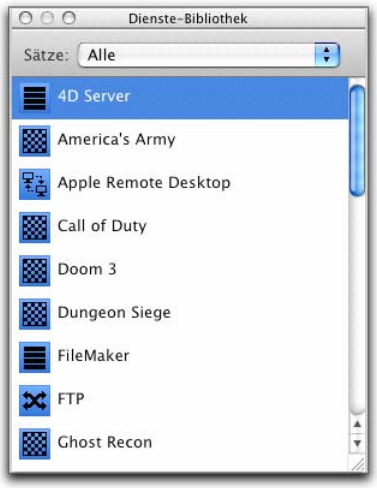
So erstellen Sie Dienste-spezifische Regeln schnell

Sie können auf zwei verschiedene Arten schnell Regeln erstellen, um den Informationsfluss zu und von bekannten Diensten und Programmen zu kontrollieren. Klicken Sie entweder auf die Schaltfläche „+“ unterhalb der Regelliste und halten Sie Ihre Maustaste eine Sekunde lang gedrückt. Sie können dann in einer Popup-Liste aus den am häufigsten gebrauchten Diensten wählen. Dann wird eine Regel, die Ihre Auswahl verwaltet, in der Regelliste angezeigt.

Oder Sie erstellen Dienste-spezifische Regeln schnell über die Dienste-Bibliothek. Wählen Sie „Fenster > Dienste-Bibliothek“ oder drücken Sie Wahltaste-Befehlstaste-S, um sich die Dienste-Bibliothek anzeigen zu lassen.



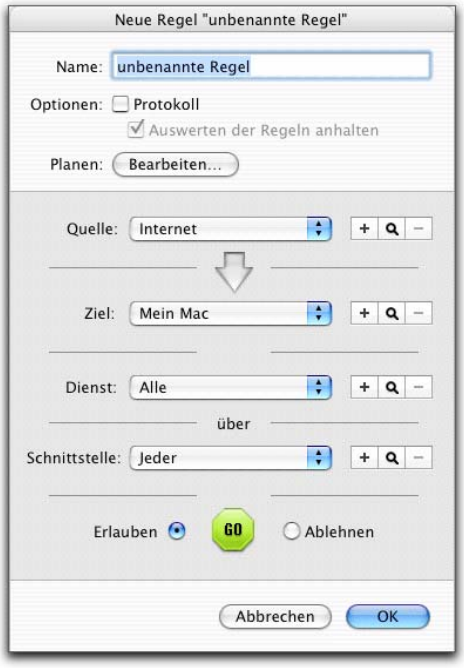
Das Fenster für die Dienste-Bibliothek wird daraufhin geöffnet und zeigt eine Liste der am häufigsten verwendeten Dienste an.



Wenn Sie eine neue Regel erstellen möchten, wählen Sie den gewünschten Dienst aus und ziehen Sie ihn in die Regelliste. Standardmäßig erlauben auf diese Weise hinzugefügte Regeln jeden Datenverkehr von Ihrem Mac zum Internet, über alle Schnittstellen. Anders gesagt: Die Regel verbietet keinerlei Aktivität solange Sie die Einstellungen nicht wie zuvor beschrieben bearbeitet haben.

Regeln manuell erstellen

Im Dialogfeld für das Ändern von Regeln können Sie auch einzelne Regeln erstellen. Klicken Sie auf die Schaltfläche „+“ unterhalb der Regelliste. Daraufhin wird Ihnen der Regel-Editor angezeigt.

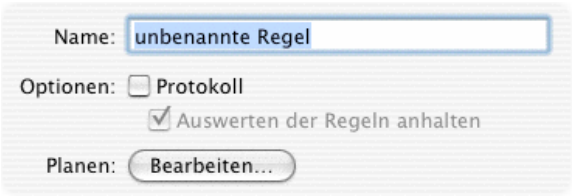


In diesem Dialogfeld können Netzwerkverwalter auf einfachste Weise einen Satz von Firewall-Regeln definieren, um die Computer in dem von ihnen betreuten Netzwerk optimal vor Eindringlingen zu schützen. Der Editor ist extrem flexibel und Sie können innerhalb von Sekunden eine unbegrenzte Anzahl von Regeln erstellen. Zum Erstellen einer Regel müssen Sie Einzelheiten in sechs Bereichen festlegen:

- **Regelname, Protokollierung und Zeitplan**
- **Regelquelle**
- **Regelziel**
- **Regeldienst**
- **Regelschnittstelle**
- **Regelaktion**

Regelbenennung, Protokollierung, Auswertung und Zeitpläne

An der Oberseite des Regel-Editors befindet sich ein Textfeld, in das Sie den Namen der Regel eingeben können. Direkt darunter befindet sich das Kontrollkästchen für das Protokoll. Wenn Sie das Kästchen für das Protokoll markieren, wir jedes Mal, wenn diese Regel aktiv wird, ein Eintrag in das Protokoll von NetBarrier X5 geschrieben. Ein kleiner roter Punkt rechts neben dem Namen der Regel in der Regelliste zeigt an, dass die Regel protokolliert wird. Wenn dieses Kontrollkästchen nicht markiert ist, wird die Regel nicht protokolliert.



Wenn das Kontrollkästchen für das Protokoll markiert ist, steht das Kontrollkästchen „Auswerten der Regeln anhalten“ zur Verfügung und ist standardmäßig markiert. Diese beiden Einstellungen bieten zusammen eine leistungsstarke Möglichkeit, um Probleme in einem Netzwerk zu beheben, ohne den Datenverkehr zu behindern.

> ACHTUNG: Wenn Sie nicht herausfinden können, warum einige Ihrer Regeln keine Auswirkungen haben, sehen Sie sich die Regeln darüber an und überprüfen Sie, ob das Kontrollkästchen „Auswerten der Regeln anhalten“ für jede dieser Regeln deaktiviert ist.

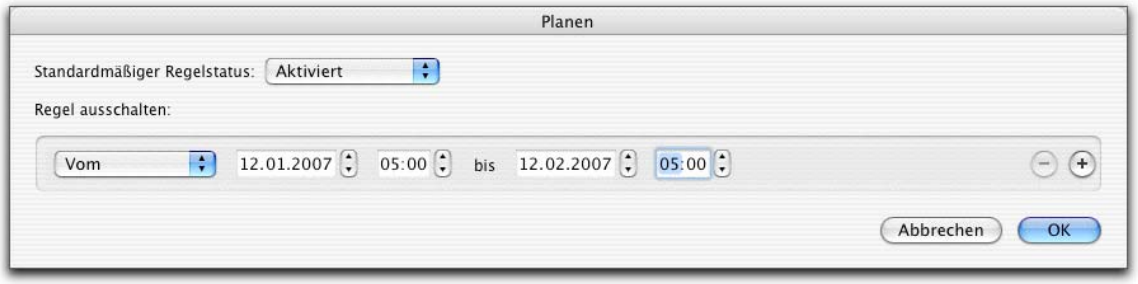
Klicken Sie zum Bearbeiten des Zeitplans auf die Schaltfläche „Bearbeiten...“. Hierauf wird das Fenster „Planen“ geöffnet.

Der Regelstatus ist standardmäßig auf „Aktiviert“ eingestellt. Das heißt, Ihre Regel ist eingeschaltet. Wenn Sie den Status auf „Abgeschaltet“ einstellen, wendet NetBarrier X5 diese Regel nicht an. Das Kontrollkästchen „Aktiviert“ ermöglicht es auch, bestimmte Regeln in eine Konfiguration aufzunehmen, aus anderen aber auszuschließen. Weitere Informationen über das Verwenden von Konfigurationssätzen finden Sie im Kapitel 10, **Einstellungen und Konfigurationen**.

Wenn Ihr Regelstatus standardmäßig eingeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel ausgeschaltet wird. Wenn Ihr Regelstatus standardmäßig ausgeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel eingeschaltet wird.

Wenn Sie das erste Mal eine Regel erstellen, ist der Regelstatus standardmäßig auf „Aktiviert“ und das Menü zum Ausschalten der Regel ist auf „Nie“ eingestellt. Anders gesagt: Wenn Sie keine weiteren Änderungen vornehmen, ist die Regel immer aktiviert. Wenn Sie die Regel für bestimmte Zeitpunkte ein- oder ausschalten möchten, klicken Sie entweder auf das Popup-Menü für „Regel aktivieren“ oder „Regel ausschalten“. Je nachdem, welchen standardmäßigen Regelstatus Sie gewählt haben. Wählen Sie dann einen der Zeitintervalle aus der Liste.

Außer der Option „Nie“ werden noch drei weitere Optionen angeboten. Mit den Optionen „Jede Woche“ und „Jeden Tag“ können Sie festlegen, ob die Regel zu einem festen, wiederkehrenden Zeitpunkt jede Woche oder jeden Tag oder an bestimmten Tagen der Woche ein- oder ausgeschaltet werden soll. Mit der dritten Option „Vom“ können Sie die Regel für einen bestimmten Zeitraum ein- oder ausschalten. In diesem Fall müssen Sie im Feld „Vom“ das Datum und die Uhrzeit festlegen, wann Ihre Regeln aktiviert werden soll. Geben Sie in das Feld „bis“ den Zeitpunkt ein, zu dem die Regel deaktiviert werden soll.

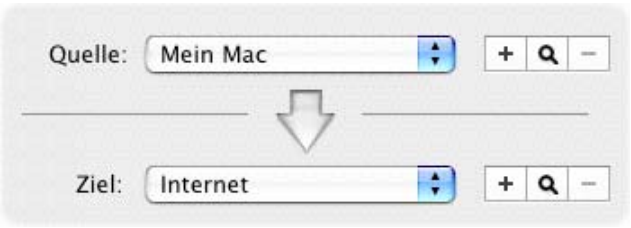


Sie können zusätzliche Zeitpunkte zum Ein- und Ausschalten der Regeln hinzufügen, indem Sie die Schaltfläche „+“ verwenden. Wenn Sie beispielsweise möchten, dass eine Regel nur montags und dienstags ausgeschaltet werden soll, können Sie diese beiden Tagen im Fenster „Planen“ festlegen. Klicken Sie auf die Schaltfläche „–“ neben der Zeile für die Zeit, um eine geplante Uhrzeit aus der Liste zu entfernen.

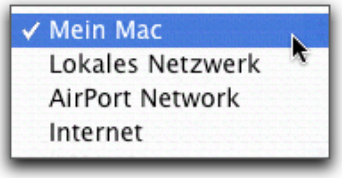
Geplante Regeln werden in der Regelliste mit einem Kalender-Symbol versehen. Für diese bestimmte Regel wurde ebenfalls die Protokollierung eingeschaltet, wie der kleine rote Punkt neben dem Namen anzeigt.

Regelquellen- und ziele

Wenn Sie Regeln festlegen, ist die Quelle das Element, das die Daten sendet. Das Ziel ist das Element, an das die Daten gesendet werden. Für jede Regel können Sie aus einer Liste mit vier Quellen und Zielen wählen. NetBarrier X5 ermöglicht es Ihnen aber nicht, für eine bestimmte Regel den gleichen Computer als Quelle und Ziel zu wählen.



Standardmäßig stehen diese vier Arten von Datenquellen und -zielen zur Verfügung:



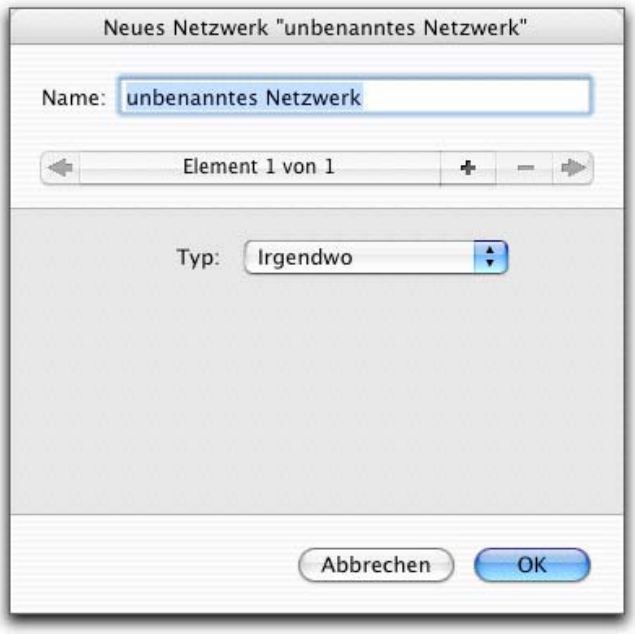
Mein Mac	Ihr Computer.
Lokales Netzwerk	Ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.
Airport-Netzwerk	Ein kabelloses AirPort-Netzwerk, mit dem Ihr Computer verbunden ist.
Internet	Das Internet (zusätzlich zu jedem lokalen Netzwerk, mit dem Ihr Computer verbunden sein kann - also alle Netzwerke).

So erstellen Sie neue Quellen und Ziele

Sie können neue Datenquelle und -ziele für die Verwendung in Ihren Regeln definieren. Damit können Sie exakt angeben, mit welchen Computern Ihr Mac kommunizieren darf.

Wenn Sie eine neue Datenquelle erstellen möchten, klicken Sie auf die Schaltfläche „+“ rechts neben dem Popup-Menü für Datenquellen oder -ziele. In unserem Beispiel erstellen wir eine neue Quelle. Sobald diese jedoch erstellt wurde, wird sie ebenfalls in der Liste der möglichen Ziele angezeigt.

Nun wird der Editor für neue Netzwerke geöffnet.



Geben Sie einen Namen ein, der Ihnen hilft, Sie an das Netzwerk zu erinnern. Wenn Sie beispielsweise IP-Adressen sperren, deren letzte acht Ziffern sich zwischen 100 und 155 bewegen, können Sie die Quelle/das Ziel „IPs von 100-155“ nennen.

Aus einem Popup-Menü können Sie sieben verschiedene Netzwerktypen wählen.

Name	Beschreibung	Adresstyp
Irgendwo	Jedes Netzwerk.	Keines, da diese Quelle alle Netzwerke abdeckt.
Mein Mac	Ihr Computer.	Die IP-Adressen von Ihrem Mac werden im Adressfeld angezeigt und können nicht geändert werden.
Mein lokales Netzwerk	Das lokale Netzwerk, mit dem Ihr Computer verbunden ist.	Die IP-Adressen von Ihrem Mac und die Subnet-Maske Ihres lokalen Netzwerks werden im Adressfeld angezeigt und können nicht geändert werden.
Gerät	Eine bestimmte IP-Adresse.	Jede IP-Adresse. Wenn Sie einen Domänennamen eingeben, wird dieser von NetBarrier X5 in eine einzelne IP-Adresse aufgelöst.
Netzwerk	Ein bestimmtes Netzwerk.	Jede Subnet-IP-Adresse und Subnet-Maske. Wie im vorigen Fall löst NetBarrier X5 Domänennamen in eine einzelne IP-Adressen auf.
Adress-Reihenfolge	Eine Gruppe von IP-Adressen.	Beginnende und endende Adressen. NetBarrier X5 löst Domänennamen in eine einzelne IP-Adresse auf.
Ethernet-ID	Ein einzelner Computer der über Ethernet mit dem Netzwerk verbunden ist.	Eine Ethernet-ID als sechs Hexadezimal-Ziffern mit zwei Buchstaben.

Regeldienste

„Dienst“ bezieht sich auf eine Kombination aus Protokolltyp, verwendeten Ports und Protokoll-spezifischen Kriterien. Diese Elemente beschreiben zusammen genommen üblicherweise ein Programm oder eine Programmart, das oder die Informationen sendet und empfängt. Beispielsweise wären Informationen, die per TCP-Protokoll über Port 80 unter Verwendung von HTTP gesendet werden, ein Webdienst.

Bei der Auslieferung von NetBarrier X5 sind mehr als 50 bekannte Dienste bereits einprogrammiert. So können Sie Datenverkehr, der von einem bestimmten Typ zu sein scheint, einfach sperren (oder erlauben).

Während die meisten programmierten Dienste deutlich auf ein bestimmtes Programm abbilden, gehören einige der ausgewählten Dienste in dieser Liste, wie beispielsweise „Web“, zu einer Datenübertragungsgruppe. Hier einige dieser nicht spezifischen Dienste:

Name	Beschreibung	Einstellungen
Alle	Alle Datenübertragungen, unabhängig vom Protokoll oder Port.	Alle Protokolle auf allen Ports.
Apple Remote Desktop	Ein Programm, mit dem ein Mac-Administratior andere Macs über eine Netzwerkverbindung steuern kann.	Port 3283 über UDP.
Verbindungsdienste	Alle TCP-Datenübertragungen. Eine TCP-Sitzung unterhält eine Verbindung zwischen Computern. So ist immer klar, dass sie durch einen Mac initiiert wurde und daher vertrauenswürdig ist. Eine UDP-Sitzung hingegen ist eine Reihe von Datenübertragungen von der man nicht „weiß“, wer sie initiiert hat.	Alle TCP-Datenübertragungen auf jedem Port.
FTP	File Transfer Protocol (Dateitransferprotokoll).	TCP, Port 20 oder 21.
iChat AV	Ein Sofortnachrichtenprogramm mit Video und Sound.	Port 5060 über UDP.
IRC	Internet Relay Chat (Internet-Relaisdialog).	TCP auf Port 194 für IRC und jeder TCP-Datenverkehr zwischen den Ports 6665 und 6669, inklusive.
iTunes Music Sharing	Eine Möglichkeit, Ihre Musikbibliothek aus iTunes über ein lokales Netzwerk mit anderen gemeinsam zu verwenden.	Port 3689 über TCP.
Mail	E-Mail-Datenübertragung.	TCP Port 25 für SMTP, Port 110 für POP3, Port 143 für IMAP4, Port 220 für IMAP3, Port 389 für LDAP und Port 587 für die

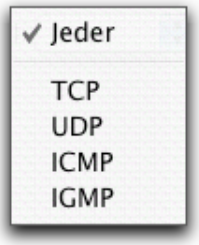
		Nachrichtenübertragung.
NTP	Network Time Protocol (Netzwerk-Zeitprotokoll).	UDP auf Port 123.
SSH	Secure Shell.	TCP auf Port 22 unter Verwendung von SSH.
Telnet	Remote-Anmeldung.	TCP auf Port 23 unter Verwendung von Telnet.
VNC	Virtual Network Computing, ein grafisches Remote-Kontrollsystem.	TCP auf Ports 5900-5999.
Web	Webbrowsen, beispielsweise über einen Browser wie Firefox.	TCP auf den Ports 80 und 8080 über HTTP und auf Port 443 über HTTPS.
Bekannte Ports	Eine große Auswahl an Ports mit einer langen Verwendungstradition bei Netzwerk-Datenübertragungen.	TCP und UDP auf allen Ports von 0 bis 1023.

Die restlichen Dienste sind nur für bestimmte Anwendungsprogramme oder Protokolle relevant.

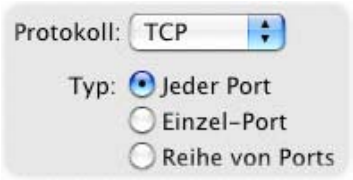
Gehen Sie beim Definieren von Regeln für bestimmte Dienste vorsichtig vor. Wenn Sie einen Dienst für ein bestimmtes Programm wählen, kann es vorkommen, dass dieses Programm den gleichen Port wie ein anderes Programm oder ein anderer Dienst verwendet. Durch das Sperren oder Freigeben eines Dienstes kann ein Konflikt mit anderen, allgemeineren Regeln entstehen. Wenn Sie beispielsweise ICQ-Datenverkehr sperren wollen, wird durch die Auswahl des Dienstes ICQ auch der Datenverkehr mit Hilfe des Programms „AOL Instant Messenger“ gesperrt, da diese beiden Programme den gleichen Port verwenden. Andere Programme verwenden unter Umständen ebenfalls die gleichen Ports. Wenn Sie erkennen, dass Sie keine Verbindung mit einem bestimmten Dienst herstellen oder keine Datenpakete senden oder empfangen können, sollten Sie die von Ihnen selbst definierten Regeln nacheinander außer Kraft setzen, um zu sehen, ob hier ein Konflikt besteht.

Definieren neuer Dienste

Aus dem Popup-Menü können Sie vier unterschiedliche Protokollgruppen wählen: TCP, UDP, ICMP und IGMP. Sie können auch die Option „Jeder“ wählen, in die sämtliche Kommunikationsprotokolle eingeschlossen sind.



Wenn Sie eine dieser Protokollgruppen wählen, werden im unteren Teil des Fensters weitere Optionen mit einer Liste der wählbaren Dienste angezeigt. Diese Optionen ändern sich je nach dem gewählten Kommunikationsprotokoll. Weitere Informationen über die Kommunikationsprotokolle und Dienste finden Sie im Kapitel 12, **Glossar**.

Protokoll	**Portauswahl**	**Optionen**
TCP oder UDP 	Jeder Port	Keine weiteren Optionen
	Einzel-Port	 (Popup-Menü enthält über 100 Optionen).
	Reihe von Ports	
ICMP oder IGMP 	Jeder	Keine weiteren Optionen
	Spezieller Typ	 (Popup-Menü enthält über 20 Optionen).

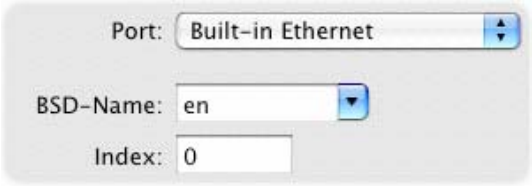
Bei allen gibt es eine Option für das Erlauben von Rundsendepaketen. Wenn dieses Kontrollkästchen markiert ist, werden Datenpakete, die an alle Computer in einem Netzwerk gesendet werden, in diesen Dienst aufgenommen.

„Ziel-Port“ ist eine letzte Option, die nur für Dienste zur Verfügung steht, die das UDP-Protokoll verwenden. Wenn diese Option markiert ist, werden Pakete entsprechend der Funktion des Ziel-Ports gefiltert. Wenn diese Option nicht markiert ist, werden Pakete entsprechend der Funktion des Quell-Ports gefiltert.

Regelschnittstellen

Eine Schnittstelle ist die Netzwerkkarte, über die Ihr Computer mit anderen Computern kommuniziert. Hierbei kann es sich um eine Ethernet-Karte, eine AirPort-Karte (für drahtlose Kommunikation Ihres Computers), eine PPP-Verbindung oder eine andere Art von Netzwerkschnittstelle handeln. Sie können aus der Liste der programmierten Schnittstellen auf Ihrem Computer wählen oder Ihre eigene Netzwerkschnittstelle definieren.

Das Popup-Menü für den Typ verfügt über zwei Optionen. Die erste Option „Jeder“ verwendet alle verfügbaren Netzwerk-Schnittstellen. Die zweite Option „Spezieller Typ“ listet die Schnittstellen auf, die für Sie zur Verfügung stehen, abhängig von der Hard- und Software Ihres Computers. Typische Schnittstellen sind folgende:

Airport Kabelloses Netzwerk	
Integriertes Ethernet Kabelschnittstelle, die üblicherweise für Netzwerkverbindungen verwendet wird.	
Integrierte FireWire-Schnittstelle Kabelschnittstelle, die üblicherweise für Peripherie-Geräte verwendet wird.	

Der BSD-Name und die Index-Nummer sind Kennungen, die von dem Unix-Layer von Mac OS X verwendet werden. Sie können diese manuell eingeben, wenn nötig. Wenn andere Schnittstellen auf Ihrem Mac vorhanden sind, steht ebenfalls die Option „Andere“ zur Verfügung.

Regelaktionen

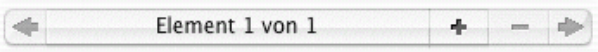
Bei Verstoß gegen eine Regel sind zwei Aktionen möglich: „Erlauben“ oder „Ablehnen“. Wählen Sie die gewünschte Aktion für Ihre Regel, indem Sie aufs entsprechende runde Optionsfeld an der Unterseite des Fensters „Ändern von Regeln“ klicken.

Klicken Sie schließlich auf „OK“, wenn Sie diese Regel zu Ihren Firewall-Regeln von NetBarrier X5 hinzufügen möchten.

Mehrteilige Quellen, Ziele, Dienste und Schnittstellen

Regelquellen, -ziele, -dienste und -schnittstellen können aus mehreren Elementen bestehen. Sie können beispielsweise festlegen, dass der Datenverkehr von mehreren bestimmten IP-Adressen verboten wird, indem Sie jede einzelne separat in einer vorhandenen Quelle auflisten.

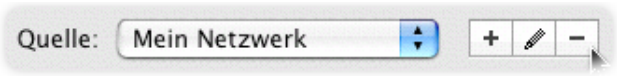
Wenn Sie eine Quelle, ein Ziel, einen Dienst oder eine Schnittstelle erstellen oder bearbeiten, wird Ihnen am oberen Fensterrand eine Leiste angezeigt, die in etwa so aussieht:



Ein neues Element erstellen	Klicken Sie auf die Schaltfläche „+“.
Zwischen den Elementen wechseln	Klicken Sie auf die Pfeilsymbole. Beachten Sie bitte, dass der Text in der Mitte Ihnen anzeigt, wo Sie sich gerade befinden und wie viele Elemente insgesamt vorhanden sind. Wenn Sie das letzte Element erreichen, können Sie mit einem Klick auf den Rechtspfeil zum ersten zurückkehren.
Ein Element löschen	Sie können ein Element nur löschen, wenn es sichtbar ist. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche „–“. Bestätigen Sie dann das Löschen in dem daraufhin angezeigten Dialogfeld.

Quellen, Ziele, Dienste und Schnittstellen löschen

Sie können von Ihnen definierte Datenquellen löschen. Wählen Sie hierzu die zu löschende Datenquelle und klicken Sie dann auf die Schaltfläche „–“.

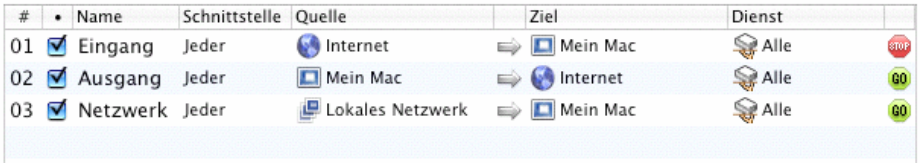


Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Netzwerk wirklich entfernen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um die Datenquelle zu löschen, und auf die Schaltfläche „Abbrechen“, um sie nicht zu löschen.

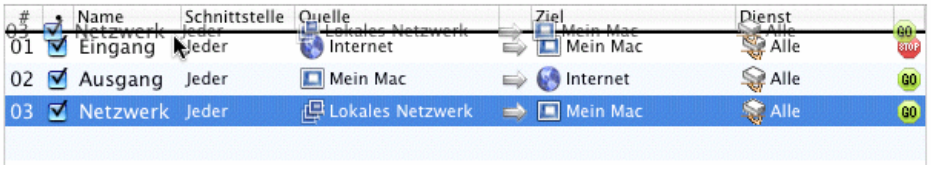
Arbeiten mit Regeln

Reihenfolge der Regeln

Die von Ihnen zur Firewall von NetBarrier X5 hinzugefügten Regeln werden von der ersten bis zur letzten ausgeführt. Damit Ihre Regeln richtig funktionieren, müssen Sie also die richtige Reihenfolge haben.



Im vorstehenden Beispiel sperrt die erste Regel vom Internet eingehende Datenpakete. Hiervon sind auch Daten betroffen, die über ein anderes Netzwerk wie z.B. ein LAN (Local Area Network = lokales Netzwerk) bei Ihrem Computer eingehen. Die Regel 3 lässt eingehende Datenpakete von einem lokalen Netzwerk zu. Da diese Regel jedoch die dritte Regel ist, wird sie nicht wirksam, da ihr die Regel 1 widerspricht. Damit die Regel 3 angewandt werden kann, muss sie in der Liste nach oben verschoben werden. Wählen Sie hierzu die Regel aus und ziehen Sie diese an die entsprechende Stelle.



Bearbeiten und Löschen von Regeln

Wenn Sie eine Regel bearbeiten möchten, müssen Sie auf den Namen der Regel und dann auf die Schaltfläche mit dem Bleistiftsymbol am unteren Rand der Liste klicken. Hierauf wird der Regel-Editor geöffnet, in dem Sie alle gewünschten Änderungen an dieser Regel vornehmen können. Klicken Sie nach Abschluss der Änderungen auf die Schaltfläche „OK“, um die Änderungen wirksam werden zu lassen. Wenn die Änderungen nicht wirksam werden sollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

Wenn Sie eine Regel löschen möchten, klicken Sie auf die Regel in der Liste mit Regeln und klicken Sie dann auf die Schaltfläche „–“ am unteren Rand der Liste.

So verwenden Sie das Kontextmenü für Regeln

In NetBarrier X5 können Sie Ihre Firewall-Regeln schnell über ein Kontextmenü ändern. Sie können dieses Kontextmenü dazu verwenden, um neue Regeln hinzuzufügen, bereits definierte Regeln zu ändern und die Eigenschaften von Regeln zu ändern.

Dieses Kontextmenü wird bei gedrückter Taste „ctrl“ geöffnet. Sie müssen nun nur noch auf den Namen einer Regel klicken. (Wenn Sie eine Maus mit zwei Tasten verwenden, können Sie auch auf die rechte Maustaste klicken, um das Kontextmenü zu öffnen.)

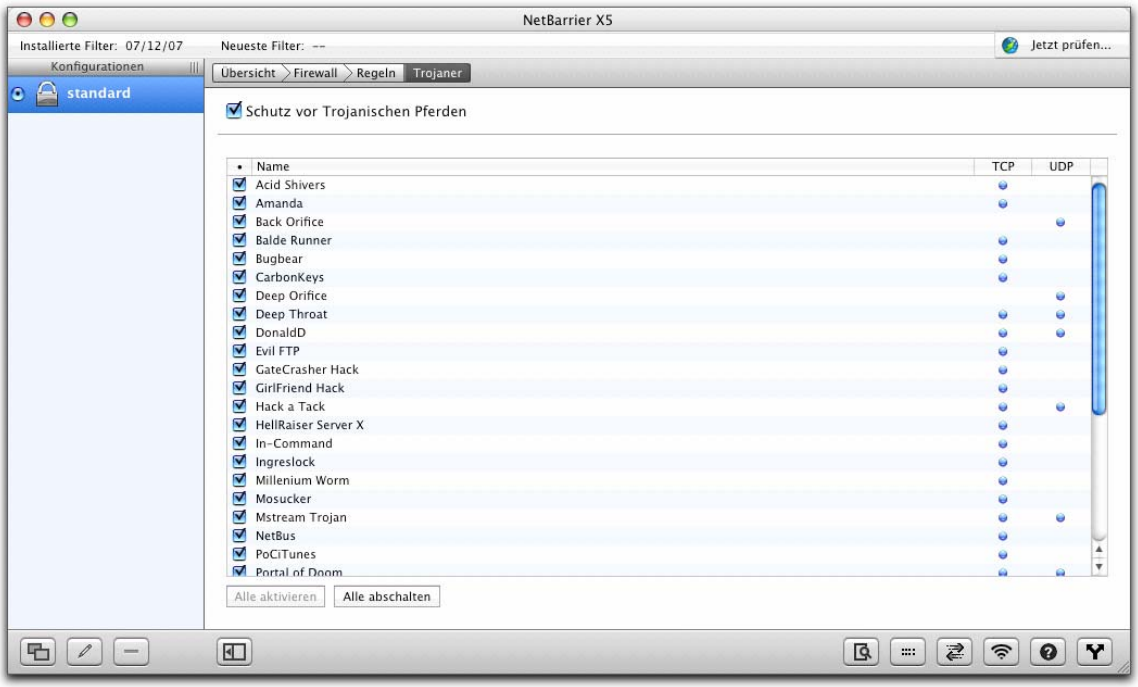
Das Menü bietet Ihnen die folgenden Optionen:

In Zwischenablage kopieren	Kopiert den Inhalt einer Regel im Nur-Text-Format in die Zwischenablage des Mac. Sie können die Regel dann in ein Dokument einfügen, wo sie dann in etwa so aussieht: „#02/EIN/Eingabe/Jede/Internet -> Mein Mac/Alle/Ablehnen“ (Schrägstriche stehen für Tabulatoren).
Standardsatz einfügen/Standardsatz hinzufügen	Fügt einen Standardsatz von Regeln aus der gleichen Auswahl, die im einfachen Modus zur Verfügung steht, ein oder hinzu: „Keine Einschränkungen“, „Kein Netzwerk“, „Client, lokaler Server“, „Nur Server“ und „Nur Client“.

Status	Sie können eine Regel aktivieren oder abschalten. Wenn die Regel so geplant wurde, dass sie zu bestimmten Zeitpunkten ausgeführt wird, wird neben „Geplant“ im Untermenü eine Markierung angezeigt.
Verhalten	Ändert das Verhalten einer Regel von Erlauben in Ablehnen des Datenverkehrs und umgekehrt.
Protokoll	Schaltet das Aufzeichnen der Datenverkehrsinformationen im Protokoll einer Regel ein und aus.
Quelle & Ziel vertauschen	„Kehrt“ eine Regel „um“, indem die Quelle und das Ziel ausgetauscht werden.
Duplizieren	Legt eine neue Kopie der Regel an.
Bearbeiten...	Öffnet den Regel-Editor für die markierte Regel.
Entfernen...	Löscht die Regel.

Schutz vor Trojanischen Pferden

Trojanische Pferde sind Programme, die heimlich auf Ihrem Computer installiert werden. Dies erfolgt entweder über virenverseuchte Anhänge, die Sie mit E-Mail-Nachrichten erhalten oder durch Programme, die Sie herunterladen oder auf einer CD kaufen. In einigen Fällen installieren Programme eine bestimmte Art von Trojanischen Pferden, die auch als Spyware bezeichnet wird. Diese sendet persönliche Informationen an einen Server. Da die Verbindung *von* Ihrem Computer hergestellt wird, gilt sie generell als vertrauenswürdig. NetBarrier X5 kann die Aktivitäten der meisten bekannten Trojanischen Pferde jedoch entdecken und stoppen. Bei den heimlich von Trojanischen Pferden gesendeten Informationen kann es sich um Informationen über das Surfverhalten des Benutzers handeln. Andere Trojanische Pferde öffnen „Hintertüren“ auf Ihrem Computer, um Hackern die Kontrolle über Ihren Computer übernehmen zu lassen, sodass dieser beispielsweise auch Dateien auf Ihrer Festplatte löschen kann.



Sie können den Schutz vor Trojanischen Pferden aktivieren, indem Sie das Kontrollkästchen zum Schutz vor Trojanischen Pferden markieren. Nun müssen Sie noch auf die Kontrollkästchen für die Trojanischen Pferde klicken, vor denen Ihr Computer geschützt werden soll. Die Schaltflächen zum Aktivieren und Deaktivieren aller Optionen am unteren Rand können Sie als praktische Kurzbefehle

verwenden, um alle Kontrollkästchen auf einmal auszuwählen oder um die gesamte Auswahl auf einmal aufzuheben.

Sie können den Schutz vor Trojanischen Pferden auch nur für ein einzelnes Trojanisches Pferd oder für alle Trojanischen Pferde aktivieren. Klicken Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen des betreffenden Trojanischen Pferds. Nun wird ein Kontextmenü geöffnet.

6 – Die vier Verteidigungslinien: Datenschutz

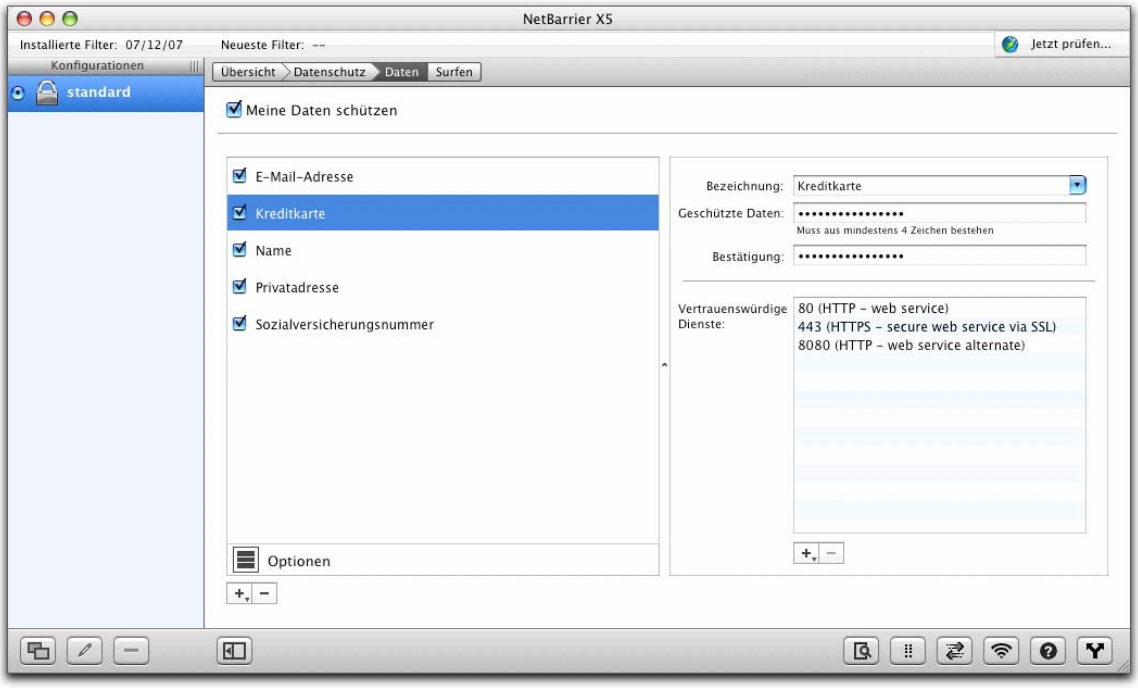
NetBarrier X5 kann ein- und ausgehende Datenpakete filtern und nach bestimmten Datentypen suchen. Es gibt mehrere Filter, die in zwei Bereiche unterteilt sind: Daten und Surfen.

Datenfilter

Der Datenfilter von NetBarrier X5 stellt sicher, dass sensible, auf Ihrem Mac gespeicherte Daten von diesem nicht über ein Netzwerk versendet werden können. Sie entscheiden selbst, welche Daten geschützt werden sollen: Ihre Kreditkartennummer, Passwörter oder Schlüsselwörter aus vertraulichen Dokumenten usw. Der in NetBarrier X5 integrierte Datenfilter überprüft jedes ausgehende Datenpaket und stellt so sicher, dass keine Dokumente versendet werden, die diese Informationen enthalten. So werden Sie nicht nur vor dem versehentlichen Versand von Dokumenten mit diesen Informationen geschützt. NetBarrier X5 sorgt auch dafür, dass niemand anderes mit einem Netzwerkzugang zu Ihrem Mac Kopien davon machen kann.

Denken Sie daran: Wenn Ihr Computer in ein Netzwerk eingebunden ist und andere Benutzer über die Datei- und Druckerfreigabe auf Ihre Dateien zugreifen können, können diese eventuell Ihre Daten kopieren.

Die folgende Abbildung zeigt das Datenfilterfenster mit einigen Beispieldaten:



So funktioniert der Datenfilter

NetBarrier X5 prüft alle Datenpakete, die von Ihrem Computer in das Internet oder in ein lokales Netzwerk gesendet werden. Wenn irgendwelche der im Filter spezifizierten Daten gefunden werden, wird das Paket blockiert.

Der Datenfilter blockiert nur die Daten, die *genau* mit dem angegebenen Text übereinstimmen, einschließlich der Satzzeichen und des Kasus. Wenn Sie beispielsweise Ihre Kreditkartennummer als zu schützende Daten angegeben haben, sorgt NetBarrier X5 dafür, dass diese Daten Ihren Computer nicht verlassen und kann Sie auf verschiedene Weise warnen, wenn Sie diese Option wählen. Wenn Sie jedoch die gleiche Nummer auf einer sicheren Webseite eingeben, verschlüsselt Ihr Browser diese Nummer. Die Daten stimmen daher nicht mehr mit den zu schützenden Daten überein und werden gesendet. Das Gleiche gilt für auf andere Weise codierte oder komprimierte Daten.

In sehr seltenen Fällen sperrt der Datenfilter Daten, die zwar mit Ihren Kriterien übereinstimmen, nicht jedoch mit Ihrer Absicht. Eine Grafikdatei (z.B. ein Bild auf einer Website) besteht im

Wesentlichen aus einer Zeichenkette, die Tausende von Zeichen lang ist. Möglicherweise kann eine Grafikdatei einen Datenteil enthalten, den Sie schützen möchten. Daher würde dieser Teil dann durch den Datenfilter gesperrt. (Wenn Sie beispielsweise den Namen „Jodie“ blockieren möchten und eine Grafikdatei die Zeichenkette „Cg34gb$sEbOJodie8%“ enthält, würde diese gesperrt. Wenn Sie feststellen, dass Sie einen bestimmten Informationsteil nicht senden oder empfangen können, schalten Sie den Datenfilter vorübergehend aus und schalten Sie ihn dann wieder ein, wenn die Informationen übertragen wurden.

Klicken Sie auf das Kontrollkästchen „Meine Daten Schützen“ in der oberen linken Ecke, um den Datenfilter zu aktivieren. Sie können diese Option jederzeit wieder deaktivieren. Beispielsweise wenn Sie vorübergehend erlauben möchten, dass Ihre geschützten Daten versendet werden.

Diese Daten können geschützt werden

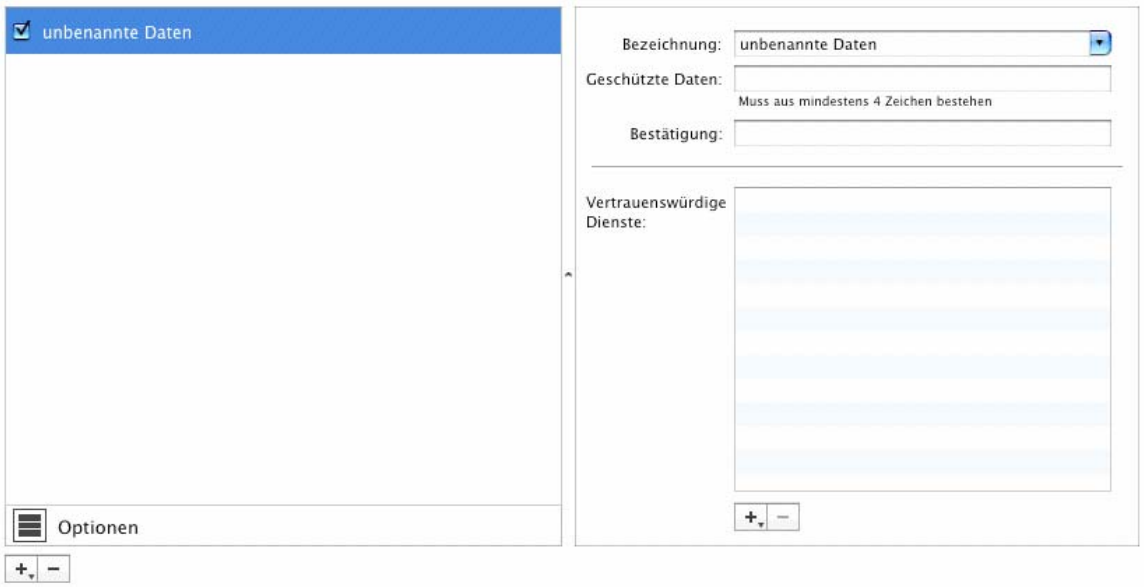
Der Datenfilter enthält Etiketten für die fünf häufigsten Arten sensibler Informationen:

- **Kreditkarten**
- **E-Mail-Adressen**
- **Privatadressen**
- **Name**
- **Sozialversicherungsnummer**

Diese Etiketten dienen jedoch nur der einfachen Handhabung. NetBarrier selbst behandelt diese Informationen nicht anders als andere oder anders als alle weiteren Informationsarten, die Sie eventuell später eingeben - beispielsweise „Telefonnummer“, „Name des Kindes“ oder „Passwörter“.

So fügen Sie dem Filter Daten hinzu

Wenn Sie dem Filter Daten hinzufügen möchten, klicken Sie auf die Schaltfläche „+“ unter dem Symbol für Optionen. Daraufhin wird in der Filterliste ein neuer Eintrag mit der Bezeichnung „unbenannte Daten“ angezeigt.

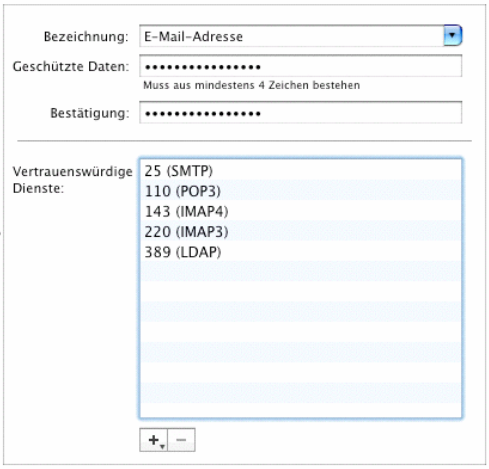


Geben Sie eine Beschreibung für Ihre geschützten Daten in das Bezeichnungsfeld ein oder wählen Sie diese aus dem Popup-Menü: Sie werden feststellen, dass diese Beschreibung in der Filterliste wiedergegeben wird. Geben Sie dann die Daten, die tatsächlich geschützt werden sollen, in das Textfeld „Geschützte Daten“ ein. Der Text wird ausgeblendet, so kann niemand sich diese Daten über Ihre Schulter ansehen oder sie bei einem späteren Zugriff auf Ihren Mac sehen. Die Daten müssen Sie dann noch einmal in das Bestätigungsfeld eingeben. Wenn die Eingabefelder für die zu schützenden Daten und die Bestätigung nicht übereinstimmen, wird ein Fenster eingeblendet, in dem Sie dann entweder die zu schützenden Daten noch einmal in beide Datenfelder eingeben oder auf die Schaltfläche „OK“ klicken können. Wenn Sie auf „OK“ klicken, müssen Sie nur das Bestätigungsfeld neu ausfüllen.

Sie müssen den Text *exakt* so eingeben, wie er in den entsprechenden Dokumenten enthalten ist. Beispielsweise kann eine Kreditkartennummer in einem Dokument im Format ####-####-####-#### oder #### #### #### #### enthalten sein. Wenn Sie Ihre Kreditkartennummer nur im ersten Format eingeben, kann Intego NetBarrier X5 Ihre Kreditkartennummer nicht schützen, wenn sie in

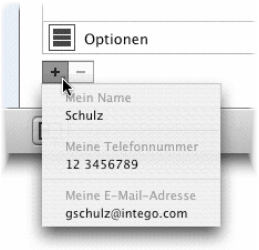
einem Dokument im zweiten Format enthalten ist. Achten Sie bei der Eingabe zu schützender Daten auch unbedingt auf korrekte Groß- und Kleinschreibweise. Wenn Sie ein Schlüsselwort wie z.B. einen Projektnamen eingeben wollen, müssen Sie dies in allen möglichen Varianten tun: Marktuntersuchung, MARKTUNTERSUCHUNG.

Im Abschnitt „Vertrauenswürdige Dienste“ können Sie auswählen, dass Daten für alle bis auf die ausgewählten Diensten gesperrt werden sollen. Klicken Sie hierzu auf die Schaltfläche „+“. Geben Sie anschließend die Port-Nummer des Dienstes ein. Alternativ können Sie auch auf das Pluszeichen klicken und die Maustaste wenige Sekunden lang gedrückt halten: Sie können dann in einer Popup-Liste aus den am häufigsten gebrauchten Diensten wählen. (Einige davon, wie beispielsweise Mail im Beispiel unten, fügen mehrere Ports auf einmal hinzu.) Sie können eine Port-Nummer oder eine Reihe von Port-Nummern hinzufügen, beispielsweise 110-123. Daten zu diesem Port (oder diesen Ports) werden nicht gesperrt. Wenn Sie andere Dienste hinzufügen wollen, müssen Sie den vorstehend beschriebenen Vorgang wiederholen. Sie können beliebig viele Dienste hinzufügen.



Sie können Dienste auch per Drag&Drop aus der Dienste-Bibliothek hinzufügen. Dies ist besonders dann hilfreich, wenn Sie die entsprechenden Port-Nummern nicht kennen, die Sie der Liste hinzufügen möchten. Wählen Sie „Fenster > Dienste-Bibliothek“ oder drücken Sie Wahltaste-Befehlstaste-S, um sich die Dienste-Bibliothek anzeigen zu lassen. Wählen Sie den gewünschten Dienst und ziehen Sie ihn auf die Liste mit vertrauenswürdigen Diensten.

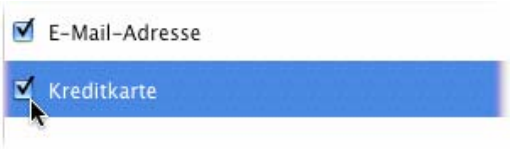
Sie können auch bestimmte persönliche Informationen von Ihrer Karte im Adressbuch von Apple hinzufügen, wenn Sie ein Feld ausgefüllt haben. Klicken Sie hierzu auf das Pluszeichen und halten Sie die Maustaste gedrückt. Daraufhin werden Ihnen drei Elemente angezeigt: Mein Name, Meine Telefonnummer und Meine E-Mail-Adresse. Wählen Sie eines der Elemente aus, um es zu den geschützten Daten hinzuzufügen.



Sobald Sie diese Informationen vollständig eingegeben haben, werden Ihre Daten geschützt. Sie können jederzeit zurückkehren, um das Datenelement zu bearbeiten. Klicken Sie hierzu in der Datenfilterliste auf das Element und ändern Sie die Informationen in dem zugehörigen Fensterabschnitt auf der rechten Seite.

So aktivieren, deaktivieren und löschen Sie Datenelemente

Jedes geschützte Objekt wird im Datenfilterfenster in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter fürs betreffende Objekt aktivieren oder abschalten. Wenn Sie ein neues Objekt hinzufügen, wird das Kontrollkästchen links davon automatisch markiert, wodurch angezeigt wird, dass der Filter für dieses Objekt aktiviert wurde. Wenn Sie diese Daten über das Internet oder ein lokales Netzwerk versenden möchten, müssen Sie das Häkchen aus dem Kontrollkästchen für das entsprechende Element entfernen. Oder Sie deaktivieren alle Datenfilter, indem Sie die Option „Meine Daten schützen“ deaktivieren, wie zuvor beschrieben.



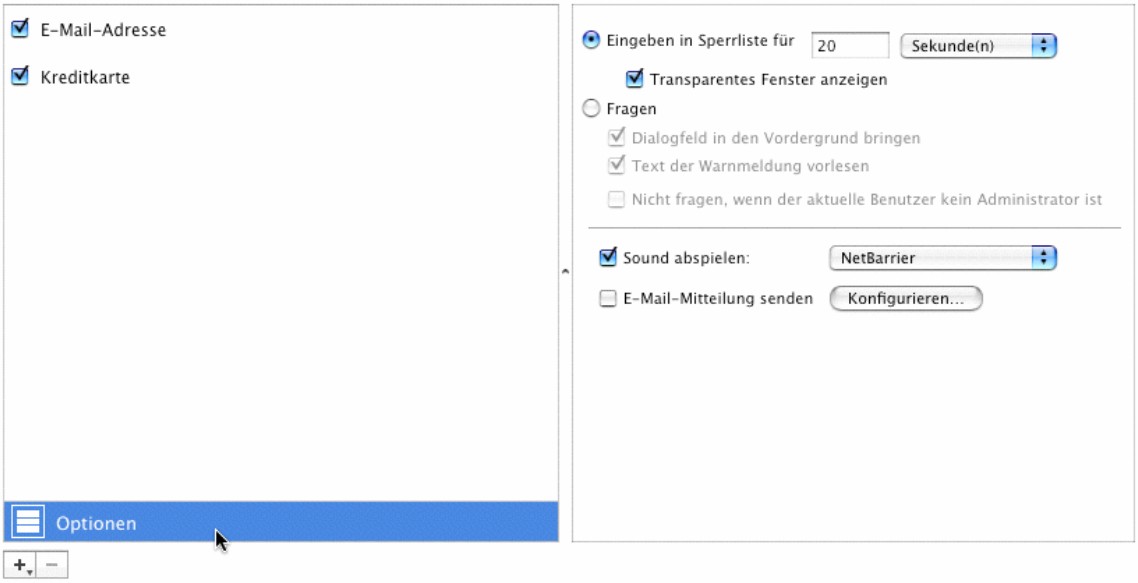
Sie können die Datenfilter für einzelne oder alle geschützten Daten aktivieren oder deaktivieren. Klicken Sie hierzu bei gedrückter Taste „ctrl“ auf der Tastatur Ihres Macintosh auf den Namen eines Datenelements oder klicken Sie mit Ihrer rechten Maustaste. Nun wird ein Kontextmenü geöffnet.

Wählen Sie die Menüoption „Abschalten“ für das gewünschte Objekt oder die Menüoption „Alle abschalten“, um den Schutz für alle Objekte zu deaktivieren. (Wenn das ausgewählte Element im obigen Beispiel bereits deaktiviert worden wäre, stünden die Optionen „Aktivieren“ bzw. „Alle aktivieren“ zur Verfügung.)

Wenn Sie das Element dauerhaft aus der Datenfilterliste entfernen möchten, klicken Sie entweder auf die rechte Maustaste, wie zuvor beschrieben, und wählen Sie „Entfernen...“ oder wählen Sie das Datenelement aus und klicken Sie dann auf die Schaltfläche „–“. In beiden Fällen werden Sie in einem Dialogfeld aufgefordert, das Löschen des Datenelements zu bestätigen.

Datenfilteroptionen

Wenn versucht wird, geschützte Daten auf Ihrem Mac zu senden oder zu empfangen, können Sie auf verschiedene Weise darüber informiert werden. Sie können auch wählen, was künftig in solchen Fällen getan werden soll. Klicken Sie auf die Schaltfläche „Optionen“ in der unteren linken Ecke des Datenfensters, um sich diese Optionen anzeigen zu lassen. Änderungen an den Datenfilteroptionen haben Auswirkungen auf alle Datenfilter.



Diese Optionen werden im Kapitel 9, **Die Bedeutung von Warnhinweisen** erklärt.

Surffilter

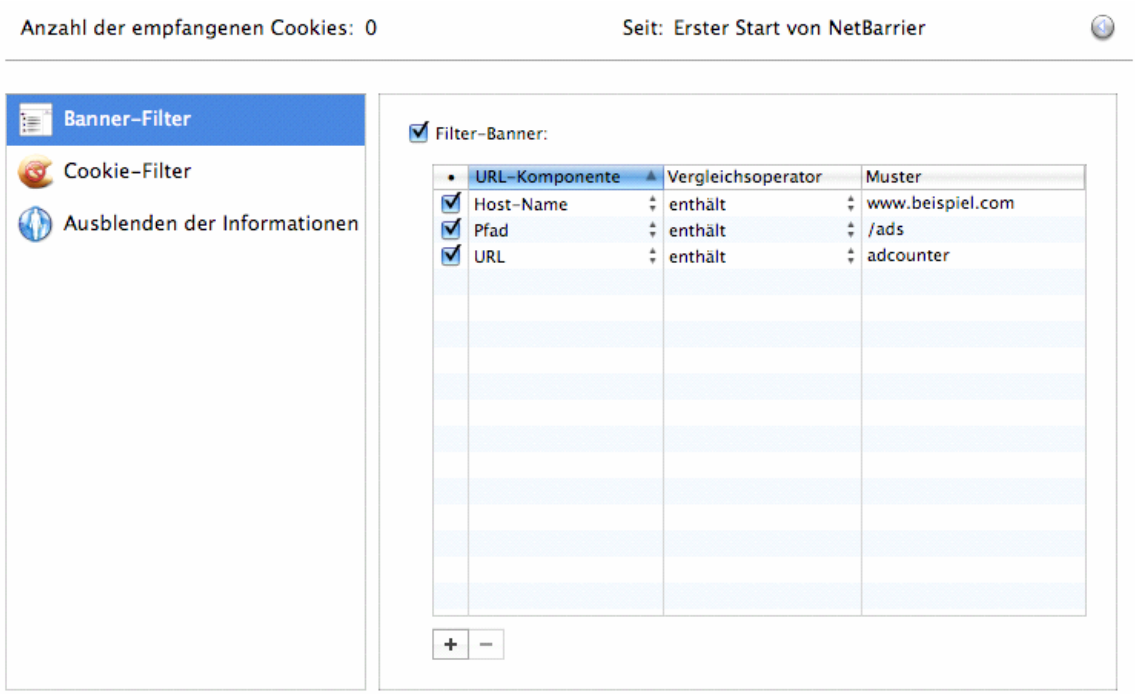
NetBarrier X5 enthält drei Arten von Filtern, mit denen Sie die Informationen kontrollieren können, die während des Surfens im Internet über Ihren Mac gesendet und empfangen werden:

- Die **Banner-Filter** blenden Werbebanner auf den von Ihnen besuchten Websites aus.
- Der **Cookie-Filter** schützt Ihren Mac vor dem Senden bestimmter Informationen an Websites, die Ihr Verhalten beobachten.
- Der Filter zum **Ausblenden der Informationen** verhüllt bestimmte Informationen über Ihren Mac: den Webbrowser, die zuletzt besuchte Website und das iTunes-Konto.

Surffilter haben Auswirkungen auf alle Computerprogramme, die Daten über HTTP übertragen (siehe Kapitel 12, **Glossar**. Webbrowser sind die bekanntesten Programme, die HTTP verwenden. Es ist jedoch ebenso Teil von iTunes, RSS-Newsreadern und vieler anderer Softwareprogramme, die über die Fähigkeit zum Internetbrowsen verfügen. Wenn Sie unerwartete Schwierigkeiten mit solchen Programmen haben - beispielsweise beim Herunterladen von Musik über iTunes -, versuchen Sie die Surffilter vorübergehend zu deaktivieren.

Bannerfilter

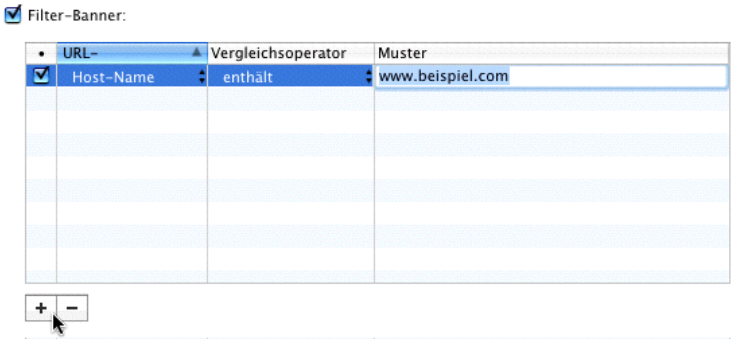
Der Bannerfilter ist eine Liste von Regeln, die NetBarrier X5 verwendet, um unerwünschtes Internetmaterial zu filtern, wie beispielsweise grafische Werbung („Werbebanner“). So wird das Surfen wesentlich schnell und ungestörter. Werbebanner werden von NetBarrier X5 gesperrt und durch kleine, transparente Grafiken ersetzt. NetBarrier X5 enthält eine interne Liste mit Werbebanner-Zeichenketten, die gefiltert werden. Sie können jedoch auch eigene Zeichenketten hinzufügen, damit noch mehr Werbung gefiltert wird, auf die Sie beim Surfen treffen. Die folgende Abbildung zeigt das Bannerfilterfenster mit einigen Beispieldaten:



Klicken sie zum Aktivieren des Bannerfilters auf das Kontrollkästchen „Filter-Banner“.

So fügen Sie Regeln für den Bannerfilter hinzu

Der Bannerfilter enthält bereits eine Reihe von Regeln, die jedes Mal aktualisiert werden, wenn Sie Ihre Filter für NetBarrier X5 mit NetUpdate X5 aktualisieren. Sie können jedoch auch einfach Ihre eigenen Regeln hinzufügen. Klicken Sie auf die Schaltfläche +, um dem Bannerfilter Regeln hinzuzufügen. So wird der Banner-Liste eine neue Zeile hinzugefügt, die Sie bearbeiten können.



Die Liste besteht aus vier Spalten: ein Kontrollkästchen, URL-Komponente, Vergleichsoperator und Struktur. Die Struktur bezeichnet offenkundig, wie Sie festlegen, was gesperrt werden soll.

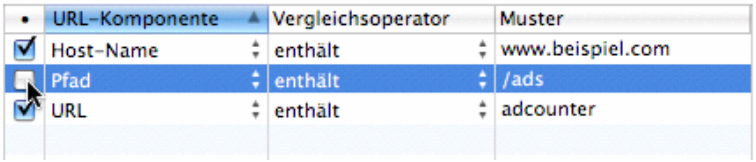
Das Popup-Menü für die URL-Komponente bietet drei Optionen. NetBarrier X5 sucht jeden Bannerfilter in dem ausgewählten Element:

Host-Name	Die Internetdomäne - also alles in einer Webadresse zwischen „http://“ und dem ersten „/“. Der Standardwert lautet „www.beispiel.com“. Beachten Sie bitte, dass ein solcher Eintrag wie „http://foren.beispiel.com“ dann (zum Beispiel) nicht gesperrt würde. Wenn Sie beides sperren möchten, sollten Sie einfach „beispiel.com“ eingeben.
Pfad	Jeden Teil der URL, der auf den Hostnamen folgt, wie z.B. /werbung/ in http://www.beispiel.com/home/grafiken/werbung/6542.html.
URL	Die gesamte URL, wie z.B. http://www.beispiel.com/home/grafiken/werbung/6542.html.

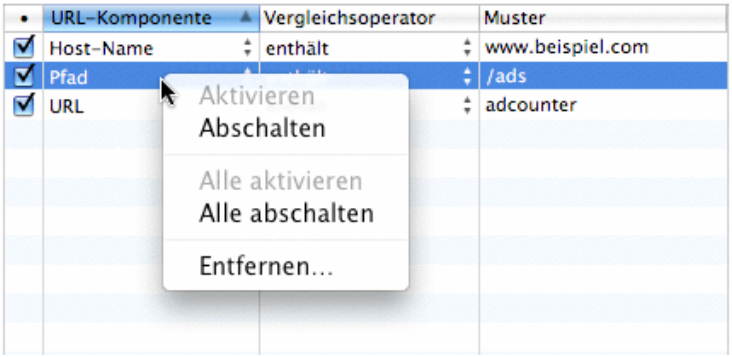
Im Popup-Menü **Vergleichsoperator** können Sie wählen, ob Inhalte auf Grund einer genauen Übereinstimmung („ist“) gesperrt werden sollen oder wenn Ihr Text mindestens mit einem Teil der URL übereinstimmt („enthält“).

So aktivieren oder deaktivieren Sie Regeln für den Bannerfilter

Jede Bannerregel wird im Bannerfenster in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter für jede Bannerregel aktivieren oder abschalten. Wenn Sie eine neue Bannerregel hinzufügen, wird das Kontrollkästchen automatisch markiert, wodurch angezeigt wird, dass der Filter für diese Regel aktiviert wurde. Wenn Sie das Sperren bestimmter Banner stoppen möchten, entfernen Sie die Häkchen aus den Kontrollkästchen für die entsprechenden Banner.



Sie können auch das Sperren von Bannern für eine bestimmte Bannerregel oder für alle Bannerregeln aktivieren. Klicken Sie hierzu bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen einer Bannerregel. Nun wird ein Kontextmenü geöffnet.



Wählen Sie die Menüoption „Abschalten“ für die gewünschte Bannerregel oder die Menüoption „Alle abschalten“, um den Schutz für alle Bannerregeln zu deaktivieren. (Wenn die Regel bereits deaktiviert war, werden die Optionen „Aktivieren“ und „Alle aktivieren“ eingeblendet).

Wählen Sie zum Entfernen von Bannerregeln entweder die Option „Entfernen“ aus dem Kontextmenü oder klicken Sie auf die Schaltfläche „–“ unterhalb der Liste mit Bannerregeln.

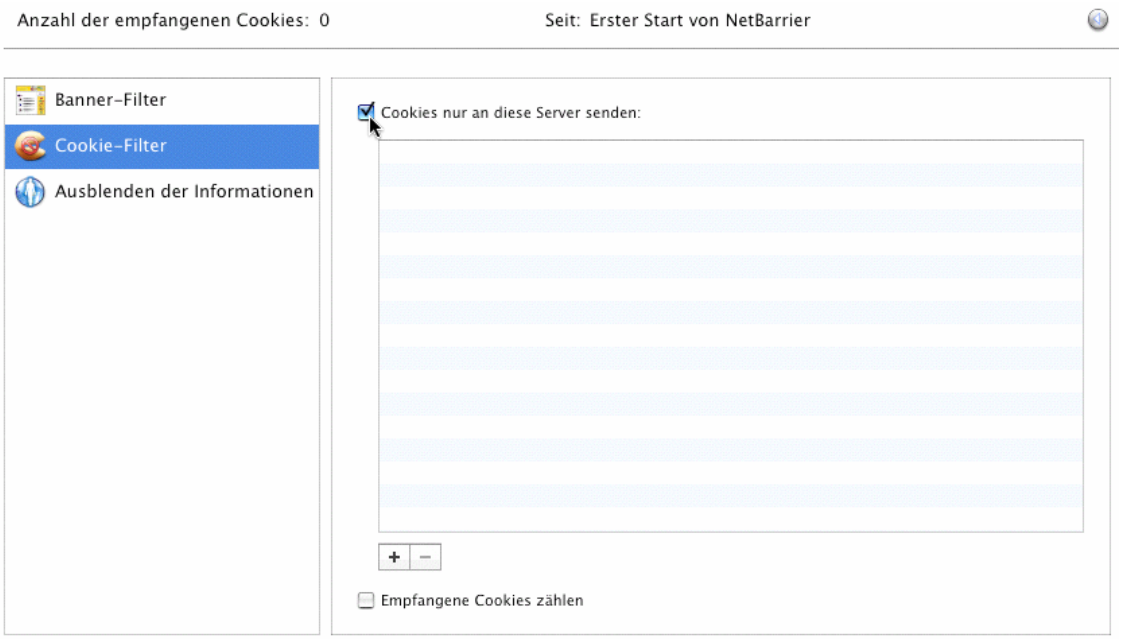
Beachten Sie bitte, dass der Bannerfilter die Inhalte nicht erkennt, die gefiltert werden, sondern nur, ob die URL mit den Kriterien übereinstimmt, die Sie festgelegt haben. Sie werden daher möglicherweise in seltenen Fällen Schwierigkeiten haben, Informationen auf einer Webseite zu sehen, die zufälligerweise mit Ihren Kriterien übereinstimmen, tatsächlich aber keine Werbebanner sind. In diesem Fall versuchen Sie, den Bannerfilter vorübergehend auszuschalten. Sie können dies aus dem Programm NetBarrier X5 heraus machen oder über das Intego-Menü in Ihrer Menüleiste.

Cookies-Filter

NetBarrier X5 enthält einen Cookie-Filter, der dafür sorgt, dass Ihr Mac keine Verfolgungsinformationen, so genannte „Cookies“, an Internetseiten senden, außer an die von Ihnen angegebenen.

Der Cookiefilter ist hilfreich, wenn Sie absolut privat surfen möchten und nur einige wenige vertrauenswürdige Seiten über Ihre Aktivitäten informieren möchten. Viele Websites - vor allem solche, für die Sie ein Passwort benötigen - funktionieren jedoch nicht richtig, wenn Sie sie nicht ausdrücklich in die Liste vertrauenswürdiger Seiten aufnehmen.

Wenn Sie den Cookie-Filter aktivieren möchten, klicken Sie das Kontrollkästchen „Cookies nur an diese Server senden:“ an.



Wenn Sie der Cookie-Filterliste einen Server hinzufügen möchten, klicken Sie auf die Schaltfläche „+“. Daraufhin wird eine Muster-Serveradresse (www.beispiel.com) angezeigt: Geben Sie anstelle dieser Adresse die Seite Ihrer Wahl ein.

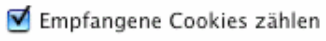
Löschen Sie die Muster-Serveradresse und geben Sie den Namen des Servers ein, dem Sie es gestatten möchten, Ihnen Cookies zuzusenden. Sie können auch eine URL aus einem Browser oder sogar eine URL im Textformat in dieses Feld ziehen, um die Adresse der Liste hinzuzufügen.

Genau wie bei den Bannerfiltern können Sie einzelne Cookie-Filter aktivieren oder deaktivieren. Klicken hierzu jeweils auf das Kontrollkästchen daneben oder halten Sie die Steuerungstaste gedrückt, während Sie darauf klicken und verwenden Sie dann das Kontextmenü. Oder Sie klicken mit Ihrer rechten Maustaste darauf.

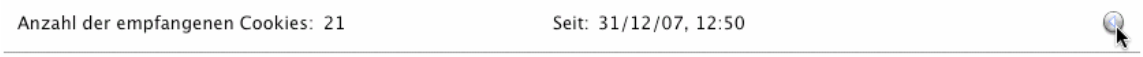
Wenn Sie Cookies löschen möchten, die bereits auf Ihrem Mac sind, lesen Sie im Handbuch für Intego Washing Machine nach, das mit NetBarrier X5 geliefert wurde.

Cookie-Zähler

NetBarrier X5 kann auch die Anzahl der an Ihren Mac gesendeten Cookies zählen. Hierzu müssen Sie nur das Kontrollkästchen **Empfangene Cookies zählen** am unteren Rand des Cookie-Filterfensters markieren.

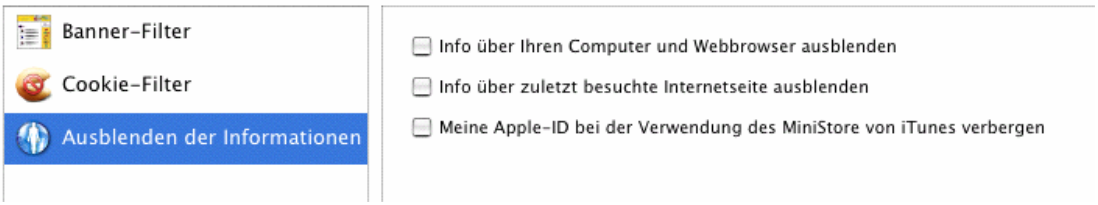


Eine Anzeige am oberen Fensterrand informiert Sie darüber, wie viele Cookies Ihr Mac akzeptiert hat, seitdem Sie den Zähler eingeschaltet oder das letzte Mal zurückgesetzt haben. Sie können den Zähler jederzeit auf Null zurücksetzen, indem Sie auf den kleinen Pfeil in der oberen rechten Ecke klicken.



Ausblenden der Informationen

Alle Webbrowser reagieren auf Anfragen von Websites, mit denen festgestellt werden soll, welches Betriebssystem (Macintosh, Windows, Linux usw.) und welchen Webbrowser und welche Version Sie verwenden. Diese Information kann dazu beitragen, dass eine Seite Informationen auf die beste Weise verbreiten kann. So können beispielsweise nur die Funktionen eingeschaltet werden, die mit dem Webbrowser funktionieren, den Sie verwenden. Andererseits beschränken einige Seiten den Zugriff aber auch auf bestimmte Plattformen und Browser. Manchmal wird der Zugriff für alle verboten, die einen Mac verwenden. NetBarrier X5 kann einige Informationen über Ihren Computer verbergen. So können Sie Zugriff auf Seiten erhalten, die Sie andernfalls nicht ansehen könnten.



NetBarrier X5 kann auf diese Anfragen antworten und nur generische Informationen senden. So kann Ihr Computer beispielsweise einer Website antworten, dass Sie einen Netscape- oder Mozillabrowser verwenden, aber ohne Versionsnummer oder Plattform. Markieren Sie hierzu das Kontrollkästchen **Info über Ihren Computer und Webbrowser ausblenden**.

Einige Websites beobachten auch, welche HTML-Seite Sie zuletzt geladen haben. Auch dies kann wiederum das Surfen im Web für Sie verbessern. Eine Einkaufsseite unterbreitet Ihnen beispielsweise bestimmte Angebote, wenn Sie von einer bestimmten Website kommen. Hemmungslose Betreiber bestimmter Seiten können diese Funktion jedoch auch verwenden, um Ihre Browseraktivitäten in einer Weise zu verfolgen, die Sie nicht möchten. Wenn Sie das Kontrollkästchen **Info über zuletzt besuchte Internetseite ausblenden** markieren, sorgt NetBarrier X5 dafür, dass Ihr Mac auf diese Art von Anfragen nicht antwortet.

Wenn Sie schließlich iTunes verwenden und sich den iTunes MiniStore anzeigen lassen, sendet iTunes Ihre Apple-ID jedes Mal an den Server von Apple, wenn Sie auf einen Song klicken. Sie können diese Funktion sperren, indem Sie **Meine Apple-ID bei der Verwendung des MiniStore von iTunes verbergen** markieren. So können Sie weiterhin Songs aus dem iTunes Store kaufen, doch iTunes wird keine Informationen mehr senden, die Ihre Browsingaktivitäten mit Ihrem Konto des iTunes Stores verknüpfen.

7 – Die vier Verteidigungslinien: Antivandalismus

Antivandalismus

Dank seiner integrierten Funktion „Antivandalismus“ ist NetBarrier X5 in der Lage, die bei Ihrem Mac eingehenden Datenpakete daraufhin zu überwachen, ob jemand versucht, in Ihren Mac einzudringen. Bei Bedarf werden diese eingehenden Datenpakete gefiltert. Die Filterung erfolgt transparent. NetBarrier X5 tritt nur dann in Erscheinung, wenn das Programm verdächtige Datenpakete entdeckt. In diesem Fall wird ein Fenster mit einer Warnmeldung geöffnet. Andernfalls überwacht die Funktion „Antivandalismus“ von Intego NetBarrier X5 kontinuierlich alle Netzwerkaktivitäten Ihres Computers im Hintergrund.

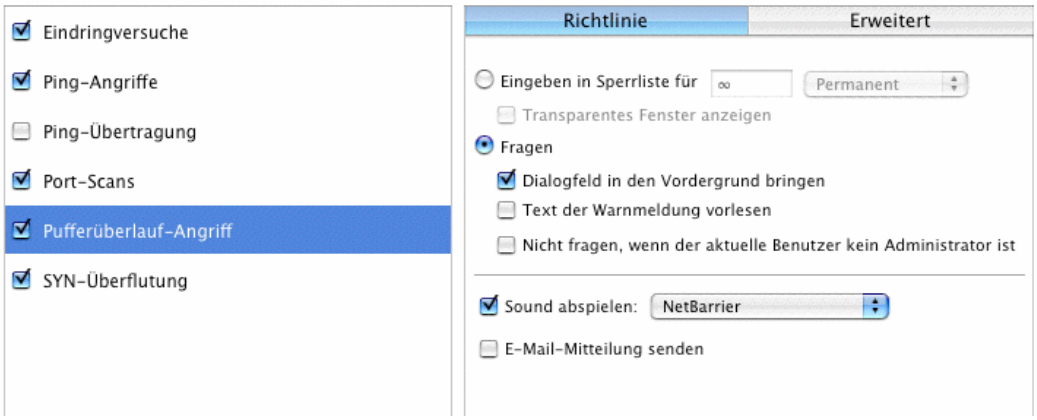
Der Abschnitt „Antivandalismus“ besteht aus zwei Teilen, die kontrollieren, wie Daten auf Ihrem Computer eingehen: Richtlinie und Anti-Spyware. Die „Sperrliste“ und die „Vertrauenswürdige Gruppe“ speichern bestimmte Hosts oder IP-Adressen, die Sie für vertrauenswürdig halten oder nicht.

Richtlinie

Der Fensterabschnitt „Antivandalismus“ bietet Richtlinienfunktionen, die vor sechs Arten des Eindringens schützen.

Pufferüberlauf-Angriff	Diese Angriffe können auftreten, wenn eine bestimmte Software Fehler beim Umgang mit Speicherplatz aufweist.
Eindringversuche	Versuche auf Ihren Mac über eine voreingestellte Anzahl von falschen Passwortanfragen innerhalb eines bestimmten Zeitraum zuzugreifen. Es gibt verschiedene Einstellungen für AppleShare IP (ASIP), FTP, HTTP, IMAP, POP und SMTP.
Ping-Angriffe	Ihr Mac empfängt eine so große Anzahl oder Frequenz von Pinganfragen, das eine Beantwortung Ihren Mac überlasten würde.
Ping-Übertragungen	Pinganfragen zur Übertragung von Adressen, wobei ein einzelner Ping über Ihr lokales Netzwerk vervielfacht wird.
Port-Scans	Versuche von Remote-Computern, die Ports Ihres Mac auf Schwachstellen zu prüfen. Wenn Sie Ihren Computer als Server einsetzen, ist es unter Umständen besser, dieses Kontrollkästchen nicht zu markieren.
SYN-Überflutung	Mehrere TCP-Anfragen, die von einem Angreifer gesendet werden, der den letzten Schritt des Austausches dann nicht vollzieht. So verbraucht der Zielcomputer Ressourcen.

Wenn Sie auf das Kontrollkästchen neben diesen Optionen klicken, wird der Schutz vor dieser Art des Eindringens aktiviert oder deaktiviert. Wenn Sie auf den Namen für den Eindringtyp klicken, werden die Richtlinien für die Benachrichtigung und die Aktion für diese Art des Eindringens angezeigt. Die folgende Abbildung zeigt beispielsweise die Richtlinie für Pufferüberlauf-Angriffe.



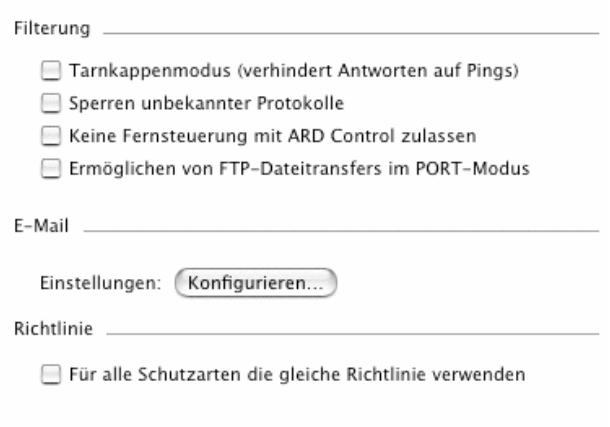
Diese Optionen werden im Kapitel 9, **Die Bedeutung von Warnhinweisen** ausführlich erklärt.

Wenn Sie auf die Registerkarte „Erweitert“ im rechten Fensterabschnitt klicken, während ein Eindringtyp ausgewählt ist, werden weitere Optionen speziell für diesen Eindringtyp angezeigt. Hierzu zählen:

Pufferüberlauf-Angriff	Keine erweiterten Einstellungen.
Eindringversuche	Sie können die Anzahl erlaubter falscher Passworteingaben für AppleShare IP (ASIP), FTP, HTTP, IMAP, POP und SMTP getrennt eingeben.
Ping-Angriffe	Die Sensibilität für Ping-Überflutung, gemessen in Millisekunden (ms), die zwischen Ping-Versuchen erlaubt ist. Wenn Ihr Computer in ein Netzwerk integriert ist, ist es vollkommen normal, dass der Netzwerkverwalter Ihren Computer gelegentlich per Ping „anbimmelt“. Andernfalls sind Pings jedoch seltener. Die einzige Ausnahme hiervon dürfte der Fall sein, wenn Sie Ihren Computer über ein DSL- oder Kabelmodem mit dem Internet verbunden haben und Ihr ISP Ihrem Computer ab und zu eine Ping-Anfrage sendet, um zu prüfen, ob Ihr Computer mit dem Kabelnetzwerk verbunden ist.
Ping-Übertragungen	Keine erweiterten Einstellungen.
Port-Scans	Die Sensibilität ist mit einem Schieberegler von niedrig bis hoch einstellbar. Die Intervalle entsprechen einer internen Berechnung.
SYN-Überflutung	Sensibilität, die in der Anzahl von Verbindungsversuchen gemessen wird, die pro Sekunde erlaubt sind.

Optionen

Im Bereich „Optionen“ der Registerkarte „Richtlinie“ stehen zusätzliche Filteroptionen zur Verfügung. Klicken Sie auf „Optionen“, um diese Einstellungen anzupassen.



Tarnkappenmodus („stealth mode“; verhindert Antworten auf Pings)	Wenn dieses Kontrollkästchen markiert ist, bleibt Ihr Computer für andere Computer im Internet oder in einem lokalen Netzwerk unsichtbar. Allerdings bleiben Sie nicht anonym: Alle von Ihrem Computer gesendeten Anfragen werden mit der IP-Nummer Ihres Computers identifiziert.
Sperren unbekannter Protokolle	Wenn dieses Kontrollkästchen markiert ist, blockiert NetBarrier X5 automatisch alle unbekannten Protokolle.
Keine Fernsteuerung mit ARD Control erlauben	Wenn dieses Kontrollkästchen markiert ist, sperrt NetBarrier X5 alle Aktivitäten von Apple Remote Desktop.
Ermöglichen von FTP-Dateitransfers im PORT-Modus	Wenn dieses Kontrollkästchen markiert ist, können Sie FTP-Dateitransfers durchführen, wenn Ihr Computer im Firewall-Modus „Nur Client“ arbeitet.

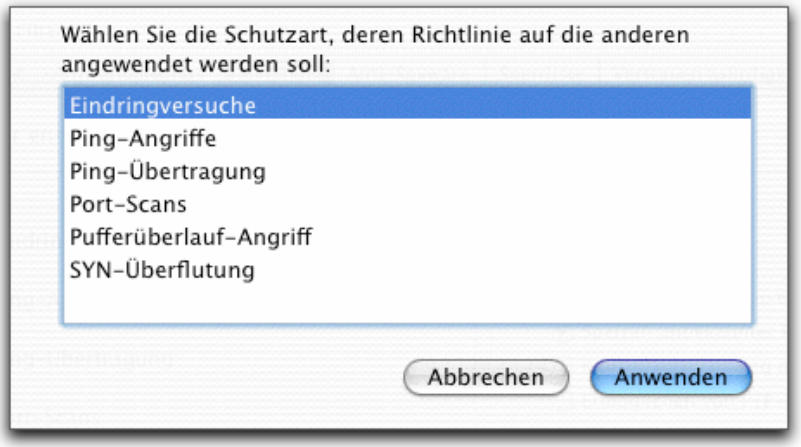
Im zweiten Teil dieses Fensters können Sie sich per E-Mail benachrichtigen lassen, wenn ein Angriff entdeckt wird. Weitere Informationen hierzu erhalten Sie in Kapitel 9, **Die Bedeutung von Warnmeldungen**.

Vereinheitlichen der Optionen für alle Richtlinien

Für jede Art des Eindringens gibt es Einstellungen, mit denen Sie festlegen können, wie Sie gewarnt werden und welche Aktionen ausgeführt werden sollen, wenn diese Art des Eindringens entdeckt wird. Diese Einstellungen werden im Kapitel 9, **Die Bedeutung von Warnhinweisen** ausführlich erklärt.

Das Kontrollkästchen „Für alle Schutzarten die gleiche Richtlinie verwenden“ vereinheitlicht alle Benachrichtigungen und Aktionen. Wenn dieses Kontrollkästchen nicht markiert ist, könnten Sie beispielsweise Folgendes auswählen: Sie erhalten eine E-Mail, wenn ein Pufferüberlauf-Angriff entdeckt wird. Wenn jedoch ein Eindringversuch stattfindet, wird Ihnen nur eine Warnmeldung anzeigt. Wenn Sie das Kästchen markieren, liefert Ihnen NetBarrier X5 bei jeder Art des Eindringens die gleiche Antwort.

Wenn Sie diese Option einschalten, wird Ihnen ein Dialogfeld angezeigt, in dem Sie die Mustereinstellungen auswählen können, die alle weiteren Eindringtypen übernehmen sollen.



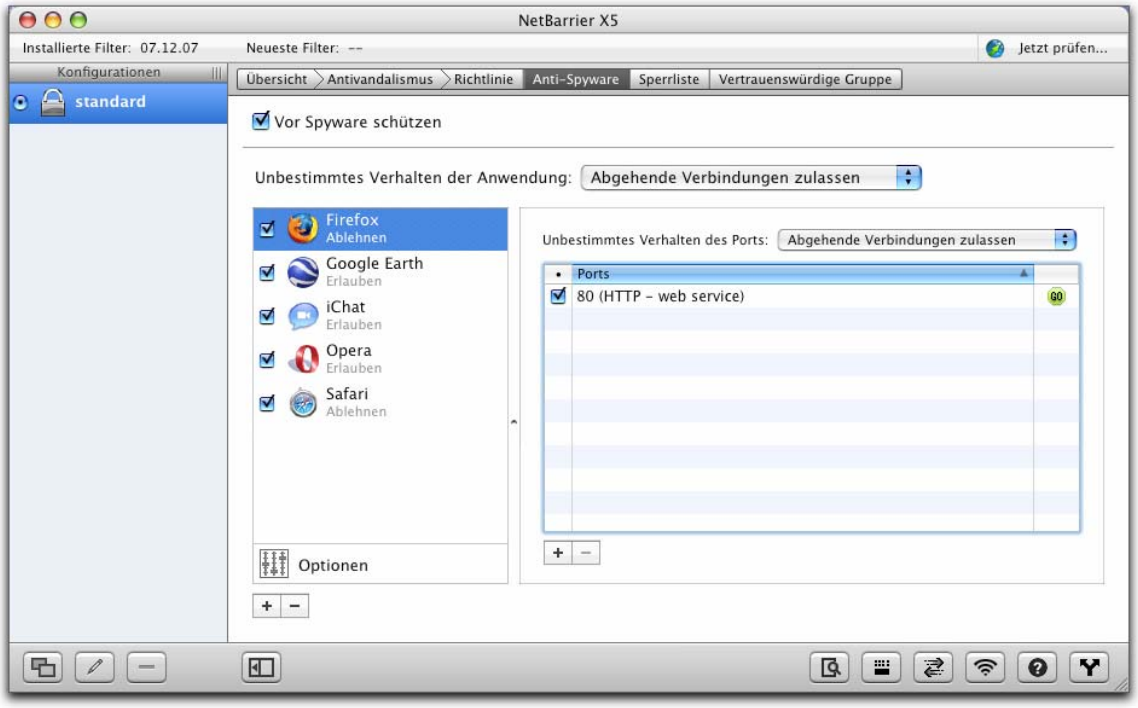
Anti-Spyware

Mit NetBarrier X5 können Sie den Zugriff einzelner Programme von Ihrem Mac aufs Internet und auf lokale Netzwerke kontrollieren. Während Ihre Firewall-Einstellungen den allgemeinen Zugriff auf Netzwerke erlauben können, ermöglichen es Ihnen die Optionen auf der Registerkarte „Anti-Spyware“, festzulegen, wie NetBarrier X5 reagieren soll, wenn bestimmte Anwendungsprogramme versuchen, auf ein Netzwerk zuzugreifen. Dies ermöglicht ihnen zweierlei:

- Wenn Sie wollen, dass bestimmte Anwendungsprogramme nicht aufs Netzwerk zugreifen können, können Sie diese auf der Registerkarte für Programme sperren.
- Wenn ein Anwendungsprogramm versucht, hinter Ihrem Rücken eine Verbindung mit einem Netzwerk herzustellen, blockiert NetBarrier X5 diesen Versuch, gibt eine Warnmeldung aus und fordert Sie auf, diesen Zugriff zu erlauben oder abzulehnen.

Auf Ihrem Mac gibt es viele Programme, die auf das Internet oder auf andere Netzwerke zugreifen. Hierzu zählen Webbrowser, E-Mail-Programme, FTP-Programme und Sofortnachrichtenprogramme (Instant Messaging). Vielleicht gibt es aber auch Programme, die eine Netzwerkverbindung herstellen, ohne Sie darüber zu informieren, um beispielsweise die Seriennummer eines auf Ihrem Computer installierten Anwendungsprogramms zu versenden, persönliche Daten über Sie zu sammeln und heimlich auf einen Server hochzuladen, oder ein Hintertürchen auf Ihrem Mac zu öffnen, sodass Hacker oder Vandalen Zugriff auf Ihren Computer erhalten. NetBarrier X5 benachrichtigt Sie über solche Versuche und gibt Ihnen die Möglichkeit zu entscheiden, ob Sie diese Versuche erlauben möchten.

Wenn Sie das Sperren von Programmen aktivieren möchten, markieren Sie das Kontrollkästchen zum Schutz vor Spyware in der oberen linken Ecke des Anti-Spyware-Fensters.

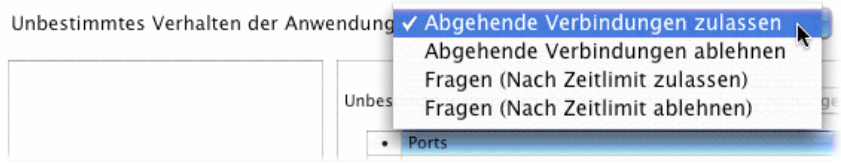


Anti-Spyware funktioniert folgendermaßen: Zuerst werden Sie gebeten, eine Liste mit Programmen zu erstellen, für die Sie die Einstellungen anwenden möchten. Diese werden als „definierte“ Programme bezeichnet, während alle Programme, die nicht auf der Liste stehen, als „undefiniert“ gelten. Im obigen Beispiel ist Google Earth definiert, während der Internet Explorer (der nicht auf der Liste steht) undefiniert ist.

Sobald Sie diese Liste erstellt haben, können Sie die Datenübertragung der definierten Programme genauer einstellen sowie eine allgemeine Richtlinie für undefinierte Programme einrichten. Zwei typische Konfigurationen wären beispielsweise folgende:

- Sie leiten ein Computerlabor und möchten, dass die Leute E-Mails mit dem Programm Mail von Apple versenden können. Sie sollen aber nicht im Internet surfen oder Netzwerkspiele spielen können. Sie würden also Mail als „Erlaubt“ definieren, aber alle ausgehenden Verbindungen anderer Programme verbieten.
- Sie vermuten, dass ein Programm, das Sie auf Ihren Mac heruntergeladen haben, unautorisiert Daten versendet - vielleicht aus einer heimlich in das Programm eingebauten Spyware. Sie definieren dieses Programm und lehnen alle Datenübertragungen aus diesem Programm ab. Datenübertragungen aus undefinierten Programmen hingegen erlauben Sie.

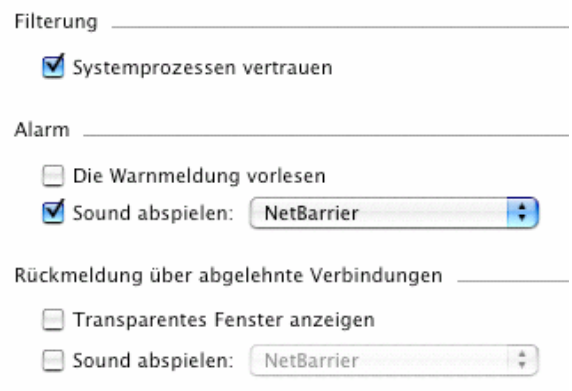
Für undefinierte Programme gibt es vier Verhaltensoptionen:



Abgehende Verbindungen erlauben	NetBarrier X5 erlaubt allen Anwendungsprogrammen den Zugriff aufs Internet und auf andere Netzwerke. Von Ihnen definierte Firewall-Regeln, womit Sie den Zugriff auf bestimmte Ports erlaubt oder gesperrt haben, bleiben jedoch in Kraft. Wenn beispielsweise ein FTP-Programm versucht, eine Verbindung mit einem Server herzustellen, wird der Internet-Zugriff durch dieses Anwendungsprogramm nicht von NetBarrier X5 gesperrt. Wenn Sie aber eine Firewall-Regel definiert haben, durch die der Zugriff auf den Port 20 (den standardmäßigen FTP-Port) gesperrt wird, so wird der Datentransfer blockiert. Wenn das FTP-Programm versucht, eine Verbindung über einen anderen Port herzustellen, wird es nicht blockiert.
Abgehende Verbindungen ablehnen	NetBarrier X5 sperrt jeden Zugriff aufs Internet und auf andere Netzwerke. Hierdurch werden alle von Ihnen definierten Firewall-Regeln außer Kraft gesetzt.
Fragen (Nach Zeitlimit erlauben)	NetBarrier X5 fragt Sie bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, ob Sie dies erlauben oder ablehnen wollen. Wenn Sie nicht innerhalb von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal gestattet.
Fragen (Nach Zeitlimit ablehnen)	NetBarrier X5 fragt Sie bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, ob Sie dies erlauben oder ablehnen wollen. Wenn Sie nicht innerhalb von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal nicht gestattet.

Optionen

Mit der Schaltfläche „Optionen“ in der unteren linken Ecke des Fensterabschnitts „Anti-Spyware“ können Sie einige allgemeine Einstellungen für Anti-Spyware konfigurieren.



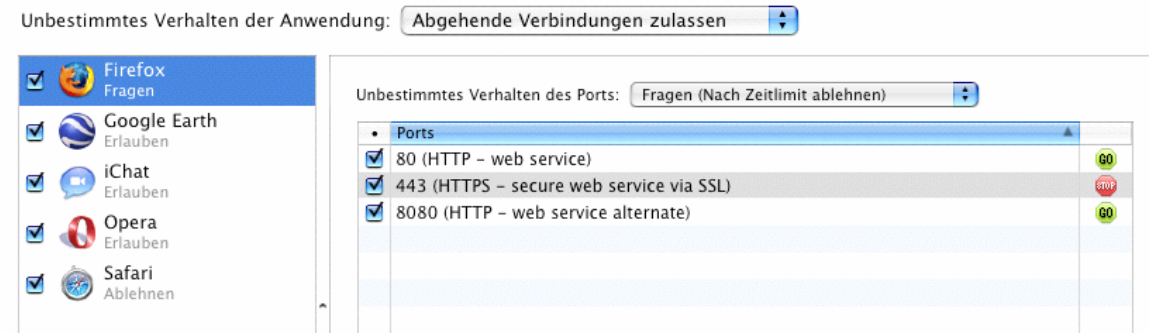
Es gibt eine besondere Option in Anti-Spyware: „Systemprozessen vertrauen“. Diese Option lässt Datenübertragungen der vielen Teile von Mac OS X selbst zu, die eine Internet- oder Netzwerkverbindung herstellen möchten. Hierzu zählen beispielsweise Druckerdienste, die Auflösung von Domänennamen, die Suche nach Software-Aktualisierungen oder die Synchronisation der Uhrzeit. Dabei handelt es sich Anfragen von Teilen von Mac OS X, nicht um separate Programme. Wenn Sie diesen Prozessen vertrauen und nicht jedes Mal gefragt werden wollen, wenn diese eine Verbindung mit dem Internet oder dem lokalen Netzwerk herstellen wollen, müssen Sie das Kontrollkästchen „Systemprozessen vertrauen“ markieren.

Weitere Informationen über andere Optionen für Anti-Spyware erhalten Sie im Kapitel 9, **Die Bedeutung von Warnhinweisen**.

Programme: Hinzufügen, Entfernen und Ändern von Einstellungen

Nachdem Sie ausgewählt haben, ob der Netzwerkzugriff von undefinierten Programme erlaubt oder abgelehnt werden soll, können Sie ein Programm definieren. Klicken Sie hierzu auf das Pluszeichen, navigieren Sie dann durch das Dialogfeld von Mac OS X bis zum Programm selbst und fügen Sie es hinzu. Wiederholen Sie diesen Vorgang für alle Programme, die Sie hinzufügen möchten. (Wenn Sie ein Programm aus der Liste löschen möchten, klicken Sie darauf und klicken Sie dann auf das Minuszeichen am unteren Rand der Programmliste).

Sie können die Einstellungen dann für jedes Programm ändern, um Datenübertragungen von dem Programm vollständig oder über bestimmte Ports zu erlauben oder abzulehnen. Ähnlich wie bei dem vorigen Vorgang, als Sie festgelegt haben, was passieren soll, wenn undefinierte Programme versuchen, Daten zu versenden, können Sie jetzt festlegen, was passieren soll, wenn ein bestimmtes Programm eine Datenübertragung von einem undefinierten Port versucht. Dann definieren Sie eine Liste mit Ports für dieses bestimmte Programm, die eine Ausnahme für die allgemeine Regel bilden.



Im obigen Beispiel:

- Fünf Programme (auf der linken Seite aufgeführt) haben bestimmte Regeln, von denen sie verwaltet werden. Ausgehende Verbindungen sind von allen anderen Programmen erlaubt.
- Firefox darf zwei Arten der Datenübertragung senden, über die Ports 80 und 8080.
- Datenübertragungen von Firefox über Port 443 sind verboten.
- Bei Datenübertragungen von Firefox über jeden anderen Port wird auf dem Bildschirm Ihres Mac ein Warnhinweis angezeigt. Wenn Sie die Datenübertragung nicht innerhalb von 90 Sekunden erlauben, wird diese verboten.

Diese Portliste besteht aus drei Spalten:

- In der ersten Spalte, die mehrere Kontrollkästchen enthält, wird das fürs Programm derzeit aktivierte Portverhalten angezeigt. Wenn das Kästchen neben einem Port markiert ist, wurde das von Ihnen festgelegte Verhalten aktiviert. Wenn Sie dieses Verhalten deaktivieren möchten, müssen Sie das Häkchen aus dem Kästchen entfernen. Sie können das Verhalten später erneut aktivieren, indem Sie das Kästchen wieder markieren.
- Die zweite Spalte mit der Überschrift „Ports“ zeigt Ihnen Informationen über die Ports an, die das Programm für den Netzwerkzugriff verwendet. Hier erfahren Sie die Port-Nummer und manchmal auch das verwendete Protokoll sowie eine kurze Beschreibung. (Diese Beschreibung wird automatisch angezeigt, wenn Sie eine Portnummer eingeben, die NetBarrier X5 erkennt). Sie können eine Port-Nummer oder eine Reihe von Port-Nummern hinzufügen, beispielsweise 110-123.
- Die dritte Spalte zeigt eines von zwei Symbol an: Ein grünes Symbol mit dem Etikett „GO“, wodurch angezeigt wird, dass der Netzwerkzugriff erlaubt wurde oder ein rotes Symbol mit dem Etikett „STOP“, wodurch angezeigt wird, dass der Netzwerkzugriff gesperrt wurde.

- Wenn Sie die Einstellung von „Erlauben“ in „Ablehnen“ ändern möchten, klicken Sie einfach auf das grüne „GO“-Symbol. Dieses verwandelt sich dann in das rote „STOP“-Symbol. Auf die gleiche Weise können Sie von „STOP“ zu „GO“ wechseln.

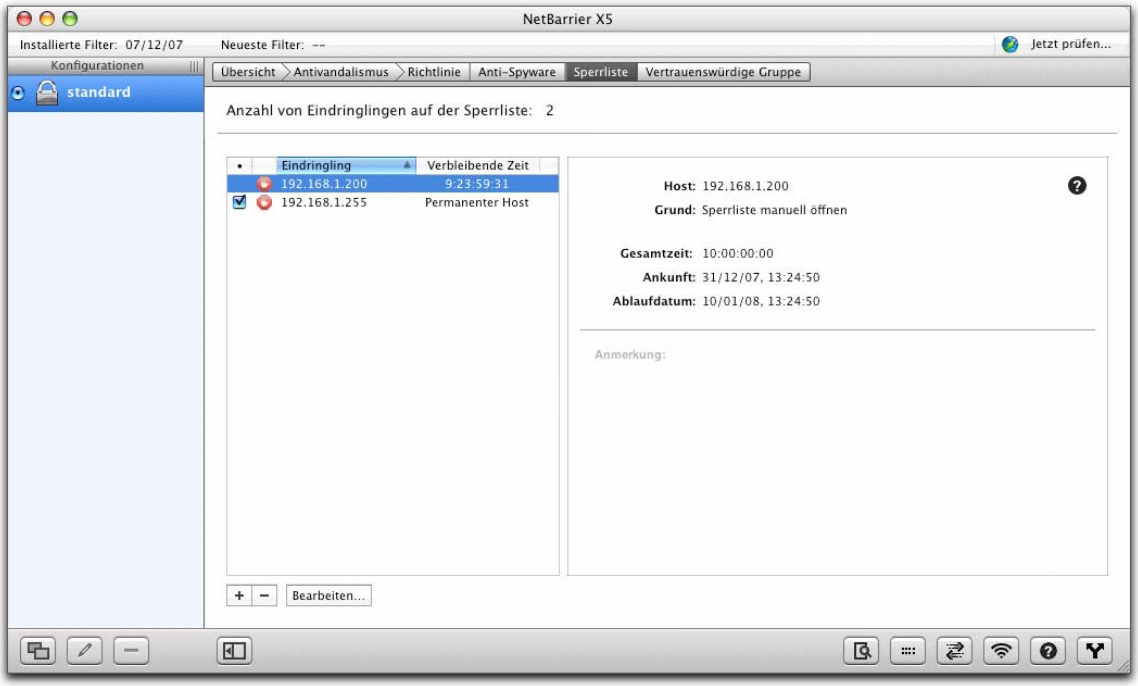
Wenn Sie sich ein Programm auf der Programmliste im Finder anzeigen lassen möchten, müssen Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf den Namen des entsprechenden Anwendungsprogramms klicken. Nun wird ein Kontextmenü geöffnet. Wählen Sie die Menüoption „Im Finder anzeigen“. Nun wird ein Fenster im Finder geöffnet, in dem Ihnen der Speicherort des Anwendungsprogramms auf Ihrem Computer angezeigt wird.

Die Sperrliste und die Vertrauenswürdige Gruppe

Die Sperrliste garantiert, dass die Datenübertragung zwischen dem Gerät eines Angreifers und Ihrem Mac, nachdem ein versuchter Angriff oder ein Eindringversuch verhindert wurde, für den von Ihnen festgelegten Zeitraum unterbunden wird.

Die Vertrauenswürdige Gruppe ist das Gegenteil der Sperrliste: Es handelt sich um eine Liste „befreundeter“ Computer, denen eine Verbindung mit Ihrem Mac *erlaubt* wird. Während die Sperrliste Sie vor „Feinden“ schützt, öffnet die Vertrauenswürdige Gruppe Ihren Freunden die Tür. Die Antivandalismus-Funktion von NetBarrier X5 sperrt den Zugriff auf Computer in der Vertrauenswürdigen Gruppe nicht und gibt auch keine Warnmeldungen über irgendwelche Aktionen aus, die von ihnen ausgeführt werden. Alle aktiven Firewall-Regeln werden jedoch auch auf die Computer in der Vertrauenswürdigen Gruppe angewendet.

Die Oberfläche des Fensters für die Vertrauenswürdige Gruppe sieht im Prinzip genauso aus, wie das Fenster für die Sperrliste. Wir untersuchen daher beide gemeinsam und heben die wichtigen Unterschiede hervor. Die folgende Abbildung zeigt das Fenster der Sperrliste mit einigen Beispieldaten.

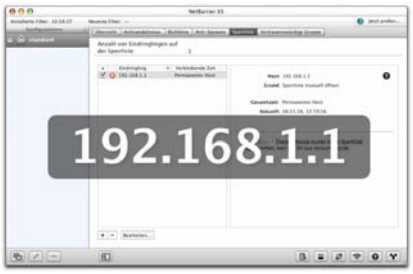


Im linken Fensterabschnitt werden Informationen über die verschiedenen IP-Adressen angezeigt, die derzeit in der Sperrliste oder in der Vertrauenswürdigen Gruppe gespeichert sind - sofern es dort welche gibt.

Kontrollkästchen	Sie können ein Element der Sperrliste/Vertrauenswürdigen Gruppe vorübergehend deaktivieren, indem Sie das Häkchen aus diesem Kontrollkästchen entfernen. Es wird standardmäßig aktiviert, wenn Sie einen Host auf eine der beiden Listen setzen. Wenn ein Element deaktiviert ist, wird es wieder aktiviert, wenn Sie darauf klicken. (Dieses Kontrollkästchen wird nur angezeigt, wenn die IP-Adresse so eingestellt ist, dass sie dauerhaft gesperrt wird.)
Eindringling/Host	Die zweite Spalte zeigt die eindringende IP-Adresse (in der Sperrliste) oder die erlaubte IP-Adresse (in der Vertrauenswürdigen Gruppe) an.
Verbleibende Zeit	Wenn Sie eingestellt haben, dass diese IP-Adresse für einen bestimmten Zeitraum verboten/zugelassen werden soll, wird in dieser Spalte angezeigt, wie viel Zeit noch verbleibt. Die Anzeige wird jede Sekunde aktualisiert. Andernfalls wird in dieser Spalte „Permanenter Host“ angezeigt. Das heißt, die IP-Adresse bleibt solange dort, bis Sie sie manuell entfernen.

Informationen über die Sperrliste/Vertrauenswürdige Gruppe

Wenn Sie auf ein Element in der Sperrliste/Vertrauenswürdigen Gruppe klicken, werden in der rechten Hälfte des Fensterabschnitts weitere Informationen angezeigt.

Host	Die IP-Adresse des Servers. Wenn Sie auf die Schaltfläche zum Überprüfen der DNS klicken (das **?**), können Sie zwischen der numerischen IP-Adresse und dem aktuellen Domänennamen des Angreifers hin- und herschalten, sofern es einen gibt. (Siehe **Hinweis zum Überprüfen der DNS**.) Sie können sich diese Adresse in großer Schrift anzeigen lassen. Verschieben Sie hierzu den Mauszeiger über das Wort „Host“. Klicken Sie mit der Maus darauf und wählen Sie aus dem Kontextmenü die Option „Große Schrift“. Das Ergebnis sieht folgendermaßen aus: 
Grund	Weshalb die IP-Nummer in die Sperrliste aufgenommen wurde. Dieser Text wird nicht im Fenster für die Vertrauenswürdige Gruppe angezeigt, da alle Elemente dort manuell hinzugefügt werden.
Gesamtzeit	Die Zeit, die eine Internet-Adresse eines anderen Computers in der Sperrliste/Vertrauenswürdigen Gruppe verbleibt. Wenn Sie auf das Wort „Gesamtzeit“ klicken, wird die Anzeige geändert und gibt die verbleibende

	Zeit an. Wenn Sie noch einmal darauf klicken wird die abgelaufene Zeit angezeigt. Sie gibt darüber Auskunft, wie lange der Angreifer bereits auf der Sperrliste steht. Wenn Sie auf „Abgelaufene Zeit“ klicken, wird Ihnen noch einmal die Gesamtzeit angezeigt.
Ankunft	Wann die IP-Nummer in die Sperrliste/Vertrauenswürdige Gruppe aufgenommen wurde.
Ablaufdatum	Wenn Sie für eine IP-Adresse einen Zeitraum festgelegt haben, über den diese in der Sperrliste/Vertrauenswürdigen Gruppe verbleiben soll, wird an dieser Stelle der Zeitpunkt angegeben, an dem sie wieder gelöscht wird.
Anmerkung	Alle Anmerkungen, die Sie für diese IP-Adresse eingegeben haben. NetBarrier X5 fügt zudem automatisch Anmerkungen hinzu, wenn das Programm ein Element in die Sperrliste aufnimmt (wie im obigen Beispiel).

Hinweis zum Überprüfen der DNS

An mehreren Stellen in NetBarrier X5 wird Ihnen ein Fragezeichen in einem dunklen Kreis angezeigt. Wenn Sie darauf klicken, können Sie sich für eine numerische IP-Adresse den zugehörigen Domänennamen anzeigen lassen und umgekehrt.

Beachten Sie bitte, dass IP-Adressen keine eindeutige Beziehung zu Domänennamen haben. Eine große Domäne kann beispielsweise „www.beispiel.com“ auf einer IP-Adresse hosten, „foren.beispiel.com“ auf einer anderen und „blog.beispiel.com“ wiederum auf einer anderen.

Kleine Domänen wiederum teilen sich eine IP-Adresse oft mit anderen, wobei alle als „virtuelle Domänen“ auf einem einzigen Computer gehostet sind. In solchen Fällen erhalten Sie beim Überprüfen einer Domäne eine IP-Adresse, die tatsächlich zu einem größeren, unerwarteten Gerätenamen führt, beispielsweise „apache2-vat.marketstreet.beispiel.com“.

Das kann dazu führen, dass durch das Eingeben einer IP-Adresse der Datenverkehr von unbeabsichtigten Domänen gesperrt (oder erlaubt) wird, während das Eingeben einer Domäne möglicherweise nicht den gesamten gewünschten Datenverkehr sperrt (oder erlaubt). Das liegt an der Beschaffenheit der Internetdomänenstruktur und ist kein Fehler von NetBarrier X5. Wenn Sie Probleme damit haben, dass Datenverkehr unerwartet gesperrt oder zugelassen wird, versuchen Sie an Stelle einer IP-Adresse einen Domänennamen zu verwenden und umgekehrt.

So fügen Sie Adressen hinzu

Sie können Adressen manuell auf zwei Arten zu einer Sperrliste oder einer Vertrauenswürdigen Gruppe hinzufügen. (NetBarrier X5 kann Adressen als Antwort auf Warnhinweise auch automatisch zur Sperrliste hinzufügen. Weitere Informationen erhalten Sie im Kapitel 9, **Die Bedeutung von Warnhinweisen**.)

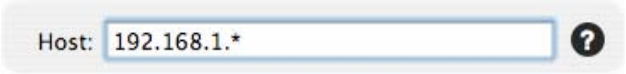
Die erste Möglichkeit besteht darin, eine IP-Adresse aus dem Protokollfenster zu wählen und dann im Kontextmenü die Option „Zur Sperrliste hinzufügen“ zu wählen. Weitere Informationen darüber erhalten Sie in Kapitel 8, **Die vier Verteidigungslinien: Überwachung**.

Sie können Adressen auch manuell der Sperrliste/Vertrauenswürdigen Gruppe hinzufügen. Klicken Sie hierzu auf das Pluszeichen am unteren Rand der Liste. Daraufhin wird ein Fenster angezeigt.

Geben Sie ins Feld „Host:“ die Adresse eines Computers ein. Wählen Sie, über welchen Zeitraum diese in der Sperrliste oder der Vertrauenswürdigen Gruppe gespeichert bleiben soll, indem Sie ins Feld „Dauer“ eine entsprechende Zahl eingeben. Wählen Sie dann eine Zeiteinheit aus dem Popup-Menü. Wenn Sie die numerische IP-Adresse des anderen Computers, die Sie in die Sperrliste aufnehmen wollen, nicht kennen, müssen Sie seinen Domänennamen eingeben und auf die Schaltfläche mit dem Fragezeichen **?** klicken. NetBarrier X5 fragt nun den DNS-Server Ihres ISP (Internet Service Provider = Internet-Dienstleister) an und trägt die korrekte IP-Nummer ins Feld ein. (Siehe **Hinweis zum Überprüfen der DNS**.) Ins Feld „Anmerkung:“ können Sie auch Anmerkungen wie z.B. den Grund für die Aufnahme der Internet-Adresse eingeben. Wenn Sie die Internet-Adresse nicht in die Sperrliste oder die Vertrauenswürdige Gruppe eingeben wollen, müssen Sie nur auf die Schaltfläche „Abbrechen“ klicken.

So verwenden Sie Platzhalterzeichen

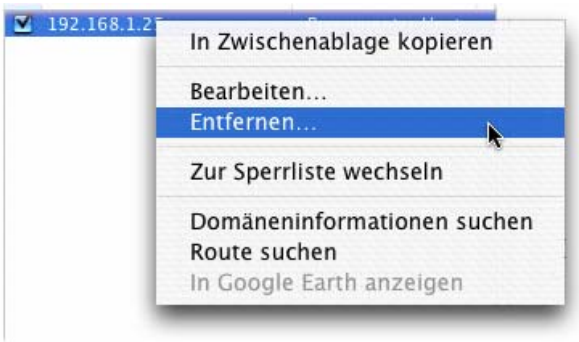
Sie können Platzhalterzeichen verwenden, um Bereiche von IP-Nummern in der Sperrliste oder der Vertrauenswürdigen Gruppe festzulegen. Geben Sie hierzu den ersten Teil der IP-Adresse ein, den Sie sperren möchten und geben Sie anschließend Sternchen ein. Die Nummer 192.168.1.* sperrt beispielsweise alle IP-Adressen von 102.168.1.0 bis einschließlich 192.168.1.255. Die Nummer 192.168.*.* sperrt IP-Adressen von 192.168.[0-255].[0-255] usw.



So entfernen Sie Adressen

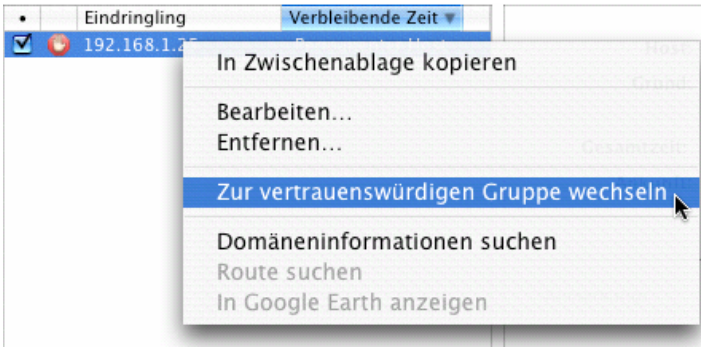
Wenn Sie eine Internet-Adresse aus der Sperrliste oder der Vertrauenswürdigen Gruppe löschen wollen, klicken Sie auf die betreffende Internet-Adresse und dann auf das Minuszeichen. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen.

Sie können eine Internet-Adresse auch löschen, indem Sie die Steuerungstaste auf der Tastatur Ihres Macintosh gedrückt halten, auf die betreffende Internet-Adresse klicken und dann aus dem Kontextmenü die Option „Entfernen…“ wählen. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen.



So verschieben Sie Internet-Adressen zwischen der Sperrliste und der Vertrauenswürdigen Gruppe

Eventuell möchten Sie eine Adresse aus der Sperrliste in die Vertrauenswürdige Gruppe verschieben oder umgekehrt. Halten Sie hierzu die Taste „ctrl“ auf Ihrer Tastatur gedrückt, wählen Sie dann die Option „Zur vertrauenswürdigen Gruppe wechseln“ oder „Zur Sperrliste wechseln“ aus dem angezeigten Kontextmenü.



So bearbeiten Sie eine Adresse

Sie können Adressen auf drei Arten in der Sperrliste oder in der Vertrauenswürdigen Gruppe bearbeiten:

- Klicken Sie auf die Adresse, die Sie bearbeiten möchten, klicken Sie dann auf die Schaltfläche „Bearbeiten“ am unteren linken Rand des Fensterabschnitts.
- Doppelklicken Sie auf die Adresse oder
- klicken Sie auf die Adresse während Sie die Steuerungstaste auf Ihrer Tastatur gedrückt halten. Wählen Sie dann „Bearbeiten...“ aus dem Kontextmenü.

Daraufhin wird der Editor für die Sperrliste/Vertrauenswürdige Gruppe angezeigt. Sie können die Adresse ändern, Anmerkungen hinzufügen oder bearbeiten oder den Zeitraum ändern, über den das Element in der Sperrliste/Vertrauenswürdigen Gruppe verbleiben soll.

Das Kontextmenü

Wie Sie bereits gesehen haben, können Sie bei gedrückter Taste „ctrl“ auf der Tastatur Ihres Macintosh auf eine Internet-Adresse in der Sperrliste/Vertrauenswürdigen Gruppe klicken. Hierauf wird ein Kontextmenü geöffnet. Es gibt vier Funktionen auf dieser Liste, die noch nicht erklärt wurden: In Zwischenablage kopieren, Domäneninformationen suchen, Route suchen und In Google Earth anzeigen.

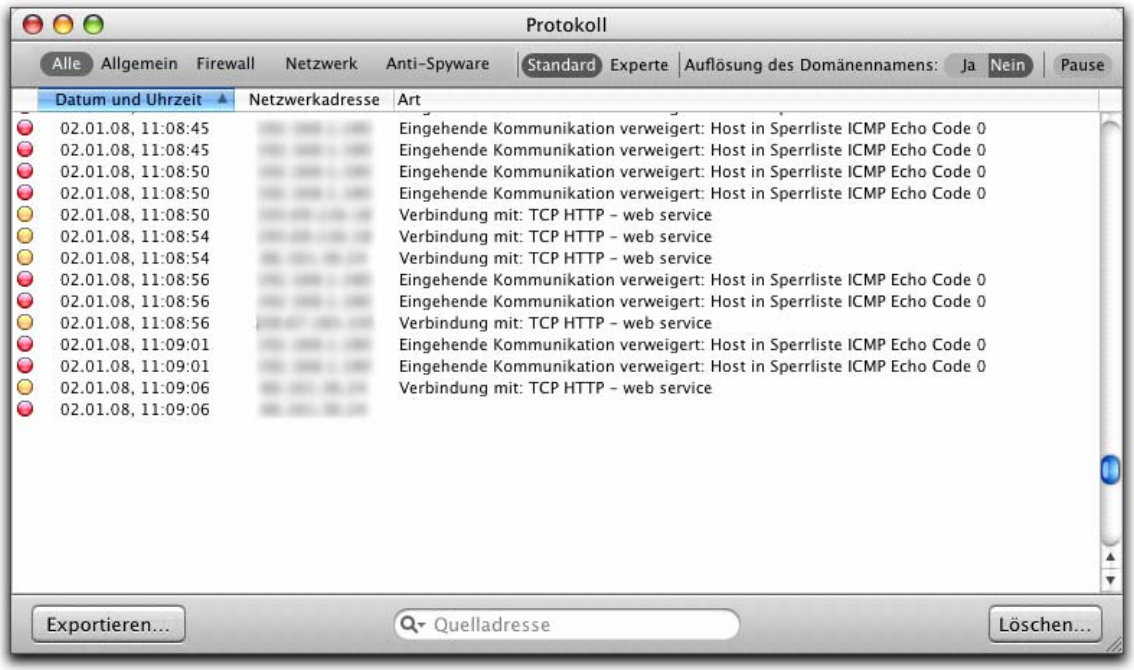
In Zwischenablage kopieren	Kopiert die IP-Adresse in die Zwischenablage von Mac OS X. Von dort aus kann sie in andere Programme eingefügt werden (z.B. in ein Texbearbeitungsprogramm).
Domäneninformationen suchen	Öffnet das Whois-Fenster von NetBarrier X5 und führt eine Suche nach der ausgewählten IP-Adresse durch. Siehe Kapitel 8, **Die vier Verteidigungslinien: Überwachung**. Dort erhalten Sie weitere Informationen.
Route suchen	Öffnet das Traceroute-Fenster von NetBarrier X5 und führt eine Suche nach der ausgewählten IP-Adresse durch. Siehe Kapitel 8, **Die vier Verteidigungslinien: Überwachung**. Dort erhalten Sie weitere Informationen.
In Google Earth anzeigen	Startet das Programm Google Earth und versucht den geografischen Ort der ausgewählten IP-Adresse zu finden.

8 – Die vier Verteidigungslinien: Überwachung

Protokoll

Im Protokoll werden alle Internet-Aktivitäten des Benutzers Ihres Computers aufgezeichnet. Im Protokoll werden alle Ereignisse, die Internet-Adressen etwaiger Eindringlinge und die Art jedes Ereignisses aufgezeichnet. Öffnen Sie das Protokoll, indem Sie auf das kleine Lupensymbol am unteren Bildschirmrand klicken. Wählen Sie dann Fenster > Protokoll oder drücken Sie Befehlstaste-Wahltaste-L.

Daraufhin wird Ihnen das Hauptfenster für das Protokoll angezeigt. Ihr Einträge unterscheiden sich selbstverständlich von den hier angezeigten. Ihre Einträge geben stattdessen die Aktivitäten auf Ihrem Mac wieder, seit Sie NetBarrier X5 installiert haben (oder seitdem Sie das Protokoll das letzte Mal gelöscht haben).



Ansichtsoptionen für das Protokoll

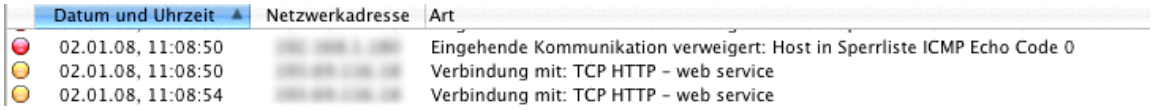
Die obere Hälfte des Protokollfensters enthält drei Optionssätze, die Auswirkungen darauf haben, wie das Protokoll angezeigt wird. Die erste Gruppe zeigt Teilsätze der Protokollaktivitäten an, durch die Sie potenzielle Probleme besser erkennen können. Die zweite Gruppe wechselt zwischen der Standardansicht und einer erweiterten Profiansicht und mit der dritten Gruppe können Sie auswählen, ob Ihnen je nach Überprüfungsvorgang der DNS die reinen IP-Adressen oder die Domänennamen angezeigt werden. Wir werden jeden dieser Sätze einzeln betrachten.

Aktivitäten fallen unter drei Gruppen: Allgemein, Firewall und Netzwerkverbindungen. Sie können sich entweder alle Aktivitäten für alle Gruppen auf einmal anzeigen lassen oder Sie lassen sich nur die Aktivitäten für eine bestimmte Gruppe an. Klicken Sie auf eine der Schaltflächen in der Schaltflächenleiste, um die Protokollansicht zu wechseln.

Alle	Alle Aktivitäten, die NetBarrier X5 verfolgt. Dies ist die Standardeinstellung.
Allgemein	Aktivitäten, die mit der Ausführung von NetBarrier X5 selbst in Verbindung stehen, wie beispielsweise Instanzen beim Starten und Beenden des Programms, zu Anti-Spyware hinzugefügte Programme, in die Sperrliste oder die Vertrauenswürdige Gruppe eingegebene Elemente usw.
Firewall	Fälle, in denen durch die Netzwerkaktivität eine Firewall-Regel aktiv wurde, sofern für diese Regel die Protokollierung aktiviert war. Aufzeichnungen über Angriffe durch ein Trojanisches Pferd werden ebenfalls im Protokoll angezeigt, sofern Sie den Schutz vor Trojanischen Pferden aktiviert haben.
Netzwerk-verbindung	Alle Verbindungen mit Netzwerken oder dem Internet, und wenn Computer mit gesperrten IP-Adressen versuchen, eine Verbindung mit Ihrem Computer herzustellen.
Anti-Spyware	Ein Teilsatz der Gruppe „Allgemein“, die nur anzeigt, wenn Programme zur Anti-Spyware-Liste hinzugefügt oder davon entfernt werden oder wenn die Anti-Spyware-Regeln zum Einsatz kommen.

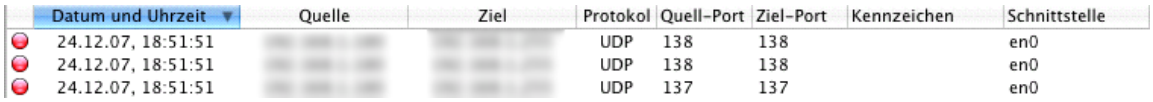
Die Protokollansichten „Standard“ und „Experte“

Standard: Die Standardansicht für das Protokollfenster Diese Ansicht zeigt nur vier Informationen für jeden Protokolleintrag an.



- Die Art der Aktivität, angezeigt durch die Farbe des Punktes:
    - Grün = Allgemein
    - Gelb = Firewall
    - Rot = Netzwerk
- Datum & Uhrzeit der Aktivität, entsprechend der Uhrzeiteinstellung auf Ihrem Mac.
- Netzwerkadresse, standardmäßig als IP-Adresse angezeigt. Wenn Sie das Kontrollkästchen „Auflösung des Domänennamens“ (siehe unten) markiert haben, sehen Sie die Domänennamen der Computer, die NetBarrier X5 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.
- Art, kurze Beschreibung der Aktivität.

Experte: Eine erweiterte Ansicht, die - sofern anwendbar - die folgenden Felder anzeigt.



- Art der Aktivität, wie zuvor beschrieben.
- Datum und Uhrzeit der Aktivität.
- Quelladresse, die IP-Nummer des Computers (oder Domäne), der die Verbindung herstellte. Für die meisten Aktivitäten wird die Quelle die IP-Adresse Ihres Macs sein. Bei Angriffen jedoch wird es die Adresse des angreifenden Computers sein. Wenn Sie das Kontrollkästchen „Auflösung des Domänennamens“ markiert haben, sehen Sie die Domänennamen der Computer, die NetBarrier X5 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.

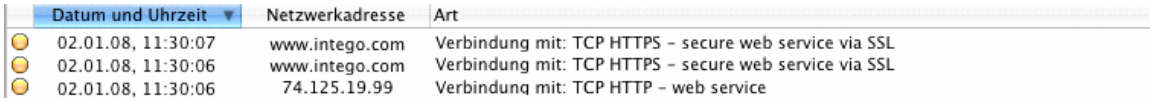
- Zieladresse, standardmäßig als IP-Adresse angezeigt.
- Protokoll das beschreibt, wie die Verbindung hergestellt werden sollte: z.B. TCP, UDP, ICMP oder IGMP.
- Quell-Port: Der Port, von dem die Daten gesendet wurden.
- Ziel-Port: Der beabsichtigte Port für die Daten.
- Kennzeichen, die TCP-Kennzeichen anzeigen: A (Acknowledge = quittieren), S (Synchronize = Synchronisation), F (end of data = Ende der Daten) oder R (Reset = zurücksetzen).
- Schnittstelle, die Netzwerkschnittstelle, die zum Senden der Daten verwendet wurde, beispielsweise Ethernet oder AirPort, durch den BSD-Namen angezeigt.
- Art, kurze Beschreibung der Aktivität.

An allgemeinen Aktivitäten, wie beispielsweise beim Starten oder Beenden von NetBarrier selbst, sind keine anderen Computer außer Ihrem Mac beteiligt. Daher sind alle Felder leer, die sich auf die Netzwerkaktivität beziehen.

Auflösung von Domänennamen

NetBarrier X5 ermöglicht es Ihnen, Eindringlinge zu verfolgen, indem Sie die Domänennamen anderer Computer auflösen. Internet-Adressen kommen in zwei unterschiedlichen Formaten vor: IP-Nummern wie z.B. 192.168.1.1 und Domänennamen wie beispiel.com. Die Beziehung zwischen IP-Nummern und Domänennamen wird von speziellen Servern (DNS, Domain Name Servers = Domänennamenserver) im gesamten Internet verwaltet.

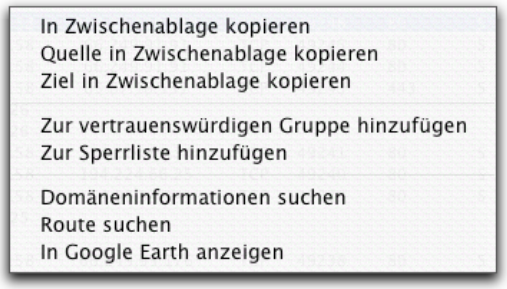
Wenn das Kontrollkästchen „Auflösung des Domänennamens“ auf der Registerkarte „Protokoll“ markiert ist, versucht NetBarrier X5, die Domänennamen aller im Protokoll enthaltenen IP-Nummern aufzulösen. Wenn NetBarrier X5 diese Informationen nicht findet, zeigt das Programm diese als Namen und nicht als Zahlen an.



NetBarrier X5 ist nicht in der Lage, die Namen aller Internetadressen aufzulösen, da nicht all diesen Adressen Domänennamen zugeordnet sind. Weitere Informationen erhalten Sie unter **Hinweis zum Überprüfen der DNS**.

Kontextmenü des Protokollfensters

Wenn Sie bei gedrückter Taste „ctrl“ auf der Tastatur Ihres Macintosh auf einen Protokolleintrag klicken, wird ein Kontextmenü geöffnet.

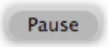


Dies enthält folgende Optionen:

In Zwischenablage kopieren	Kopiert sichtbare Spalten aus diesem Protokolleintrag in einem durch Tabulatoren getrennten Textformat in die Zwischenablage von Mac OS X. Anschließend können Sie den Inhalt der Zwischenablage in ein Dokument jedes beliebigen Anwendungsprogramms einsetzen.
Quelle in Zwischenablage kopieren	Kopiert nur das Quellfeld dieses Protokolleintrags in die Zwischenablage von Mac OS X: Steht nur zur Verfügung, wenn Sie das Protokoll im Expertenmodus ansehen.
Ziel in Zwischenablage kopieren	Kopiert nur das Zielfeld dieses Protokolleintrags in die Zwischenablage von Mac OS X: Steht nur zur Verfügung, wenn Sie das Protokoll im Expertenmodus ansehen.
Zur vertrauenswürdigen Gruppe hinzufügen	Fügt diese IP-Adresse dauerhaft der Vertrauenswürdigen Gruppe hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen erlaubt. Die Firewall von NetBarrier X5 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-Adresse angewendet.
Zur Sperrliste hinzufügen	Fügt diese IP-Adresse dauerhaft der Sperrliste hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen gesperrt. Die Firewall von NetBarrier X5 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-

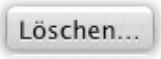
	Adresse angewendet.
Domäneninformationen suchen	Startet das Whois-Fenster von NetBarrier X5 und führt eine Suche nach der ausgewählten IP-Adresse durch. Weitere Informationen erhalten Sie unter **Whois**.
Route suchen	Startet das Traceroute-Fenster von NetBarrier X5 und führt eine Suche nach der ausgewählten IP-Adresse durch. Weitere Informationen erhalten Sie unter **Traceroute**.
In Google Earth anzeigen	Startet das Programm Google Earth, sofern Sie es installiert haben, und versucht den geografischen Ort der ausgewählten IP-Adresse zu finden. Siehe Kapitel 8, **Die vier Verteidigungslinien: Überwachung**. Dort erhalten Sie weitere Informationen.

Pausieren der kontinuierlichen Protokollanzeige



Wenn innerhalb kurzer Zeit viele Verbindungen mit Ihrem Computer hergestellt und beendet werden, kann es problematisch sein, das sich ständig aktualisierende Protokoll zu lesen. Sie können das Protokoll einfacher ansehen, wenn Sie auf die Schaltfläche zum Anhalten in der oberen rechten Ecke des Protokollfensters klicken. Das Protokoll wird angehalten, damit Sie die Daten lesen können. Das Protokoll zeichnet jedoch weiterhin Daten auf und zeigt die neuen Daten an, wenn Sie das Protokoll weiterlaufen lassen. Klicken Sie erneut auf die Schaltfläche „Pause“, um wieder die Echtzeitanzeige des Protokolls zu aktivieren.

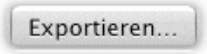
So löschen Sie das Protokoll



Um alle im Protokoll gespeicherten Informationen zu löschen, müssen Sie nur auf die Schaltfläche „Löschen…“ in der unteren rechten Ecke klicken. Nun wird ein Fenster geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen.

Das Protokoll wird auch automatisch gelöscht, wenn Sie das Kontrollkästchen „Protokoll nach dem Exportieren löschen“ in den Einstellungen für das Protokoll markiert haben und wenn Sie NetBarrier X5 so eingerichtet haben, dass regelmäßig ein Protokoll exportiert wird. Siehe Kapitel 10, **Einstellungen und Konfigurationen**.

So exportieren Sie das Protokoll



Sie können das Protokoll in mehreren Formaten exportieren. Beim manuellen Exportieren werden nur die angezeigten Daten exportiert. Wenn Sie also beispielsweise nur das Kontrollkästchen „Firewall“ auf der Registerkarte „Protokoll“ markiert haben, werden nur die Firewall-Daten exportiert. (Sie können die Protokolldaten auch automatisch exportieren lassen. Siehe Kapitel 10, **Einstellungen und Konfigurationen**.)

Sie können das Protokoll exportieren, indem Sie auf die Schaltfläche „Exportieren…“ klicken. Nun wird ein Dialogfeld geöffnet, sodass Sie die Datei speichern können. Hierbei können Sie den Namen der Datei ändern. Wählen Sie den Ort, an dem das Protokoll gespeichert werden sollen. Standardmäßig werden alle Dateien mit exportierten Daten im Ordner ~/Library/Logs/NetBarrier gespeichert.

ACHTUNG: Es kann einige Minuten dauern bis das Protokoll exportiert ist, wenn die Funktion zum Auflösen des Domänennamens eingeschaltet ist.

Protokolle können in sechs Formaten exportiert werden: Klicken Sie ins Popup-Menü „Format“, um das Exportformat zu wählen.

Dabei handelt es sich um folgende Formate:

HTML für Experten	HTML-Format das alle Spalten anzeigt, die im Expertenmodus sichtbar sind. In diesem Format können Sie den letzten Browserverlauf teilweise zurückverfolgen, da NetBarrier X5 anklickbare Links liefert für alle Versuche, nicht sichere Webseiten aufzurufen. (Das sind über TCP verbundene Ziel-Ports, die auf die Ports 80 oder 8080 zielen.)

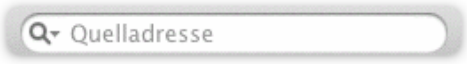
Text für Experten	Durch Tabulatoren getrenntes Nur-Text-Format mit zusätzlichen Spalten, damit im Expertenmodus alle sichtbaren Spalten angezeigt werden können. Dieser Modus eignet sich am besten zum Importieren in eine Tabelle oder ein Datenbankprogramm.
HTML	HTML-Format das alle Spalten anzeigt, die im Standardmodus sichtbar sind. Wie bei HTML für Experten-Exporten können Sie mit diesem Dateiformat den letzten Browserverlauf zurückverfolgen.
Analytisch	Ein Textformat, das dem Format „Text für Experten“ ähnelt, wobei allerdings keine Reiter vorhanden sind. Manche Felder sind beschriftet.
Text	Durch Tabulatoren getrenntes Nur-Text-Format mit allen im Standardmodus sichtbaren Spalten.
Wer ist da?	Das Protokoll als Textdatei mit den folgenden Spalten: Datum, Uhrzeit, Ergebnis, Hostname, Server-Port und Methode: hilfreich in einigen Protokollanalyseprogrammen.

Filtern von Daten im Protokollfenster

Am unteren Rand der Symbolleiste im Protokollfenster gibt es ein Suchfeld zum Filtern von Daten im Protokollfenster nach bestimmten Kriterien. Es werden dann die Einträge angezeigt, die die ausgewählten Kriterien aus den folgenden Kategorien enthalten:

- **Quelladresse**
- **Zieladresse**
- **Quell-Port**
- **Ziel-Port**
- **Schnittstelle**
- **Protokoll**

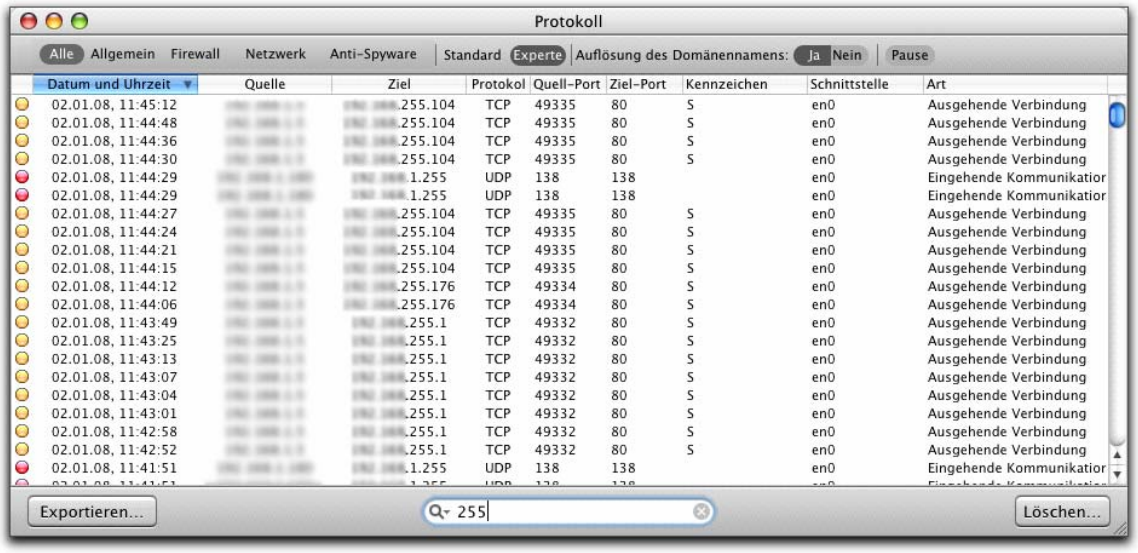
Die Quelladresse ist das Standardkriterium, wie im Suchfeld angezeigt.



Wenn Sie nach Protokolleinträgen suchen wollen, von denen dieser Kriterien erfüllt werden, müssen Sie aufs Schließdreieck neben der Schaltfläche „Suchen“ klicken.

Wählen Sie das gewünschte Suchkriterium und geben Sie eine Zeichenfolge in das Feld für die Eingabe des Suchbegriffs ein. Sie müssen nicht den gesamten Suchbegriff eingeben. Mit der Eingabe jedes weiteren Zeichens des Suchbegriffs wird die Anzahl der angezeigten Protokolleinträge entsprechend verringert.

Im Beispiel unten suchen wir nach „255“ in der Zieladresse. Der Suchtext kann an einer beliebigen Stelle im Feld auftauchen, nicht nur am Anfang. Die Suche funktioniert auch dann, wenn Sie sich das Protokoll im Standardmodus ansehen. Das Suchfeld ist dann ausgeblendet (in diesem Fall das Ziel).



Wenn Sie den Inhalt des Suchfelds löschen wollen, um eine neue Suche zu starten, müssen Sie auf die Schaltfläche mit dem kleinen „x“ im Suchfeld klicken.

Verkehr

Das Fenster für den Datenverkehr enthält einen Satz von Anzeigepegeln für die Aktivität. Er zeigt Ihnen die Art und die Anzahl der Netzwerkaktivitäten an, die sowohl über das Internet als auch über lokale Netzwerke auf Ihrem Mac ein- und ausgehen. Sie können auf das Fenster für den Datenverkehr zugreifen, indem Sie auf das kleine Symbol klicken, das unten angezeigt wird und dann „Fenster > Verkehr“ wählen. Sie können auch Befehlstaste-Wahltaste-1 drücken.

Ansichtsmodi für den Datenverkehr

Für das Datenverkehrsfenster gibt es vier Ansichtsmodi. Sie können zwischen ihnen hin- und herwechseln, indem Sie auf die kleinen Schaltflächen am oberen Bildschirmrand klicken.

Die erste Schaltfläche ist die Standardansicht und zeigt den Datenverkehr durch zwei Pegelzeilen und eine Zeitlinie an.

Die oberen Pegel „EIN“ zeigen Werte standardmäßig in Orange an und geben die Anzahl der eingehenden Daten auf Ihrem Mac wieder. Die Pegel „AUS“ in der zweiten Zeile zeigen Werte standardmäßig in Grün an und geben die Anzahl der ausgehenden Daten auf Ihrem Mac wieder. Die Zahl in den Pegeln gibt den aktuellen Datendurchsatz in Kilobyte pro Sekunden (k/s) wieder. Darunter steht die Gesamtzahl, normalerweise in Megabyte (MB) oder Gigabyte (GB).

Die Zeitachse unten zeigt den Datenverkehr im Zeitverlauf an. Die Balken ganz rechts zeigen die Gegenwart an und die linken die Vergangenheit. Wie oben zeigen die orangenen Werte den eingehenden Datenverkehr und die grünen Werte zeigen den ausgehenden Datenverkehr.

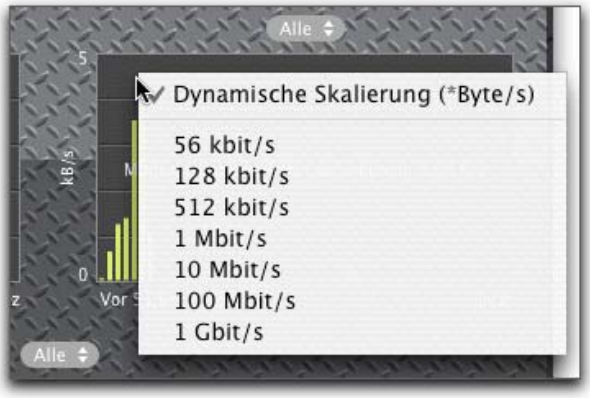
Die Zeitachse wird dynamisch skaliert: sie ändert sich in Abhängigkeit vom Datenverkehrsaufkommen. Im obigen Beispiel bewegt sich der Datendurchsatz zwischen 0 und 150 KB pro Sekunde. Die Obergrenze für das Diagramm liegt daher bei 250 KB pro Sekunde, wie man in der Legende links vom Diagramm sehen kann. Aber in diesem zweiten Beispiel ist der Datenverkehr gering und erreicht höchstens 800 *Bytes* pro Sekunde. Das sind weniger als ein Kilobyte. Die Messeinheit wechselt daher in Bytes und die Obergrenze des Diagramms liegt bei 1.000.

Standardmäßig zeichnet die Zeitachse Aktivitäten der vergangenen 111 Sekunden auf. Sie können den Zeitraum verlängern, indem Sie das Fenster größer ziehen. Klicken Sie hierzu entweder auf die grüne Schaltfläche „Maximieren“ von Mac OS X in der oberen linken Ecke oder klicken Sie auf die untere rechte Ecke des Fensters und ziehen Sie das Fenster auf. Die Maximalzeit wird durch die Größe Ihres Bildschirms festgelegt oder dadurch, ob Sie sich jeweils nur einen Bereich der Zeitachse ansehen möchten.

Wenn Sie den Mauszeiger über eine Zeitachse verschieben, wird ein Text angezeigt, aus dem der aktuelle durchschnittliche Datendurchsatz ersichtlich ist. Der Wert des Datendurchsatzes wird einmal pro Sekunde aktualisiert.

Die zweite Ansichtsschaltfläche zeigt den Datenverkehr in drei Zeitachsen an: eine für den eingehenden, eine für den ausgehenden und eine für den gesamten Datenverkehr.

Für diesen Ansichtsmodus gibt es eine Spezialfunktion, mit der Sie die Skala für die Diagramme „EIN“ und „AUS“ wählen können. Verschieben Sie hierzu die Maus über eines der Diagramme, halten Sie dabei die Steuerungstaste gedrückt und klicken Sie. Daraufhin können Sie in einem Popup-Menü aus mehreren Optionen wählen.



Damit können Sie die korrekte Skalierung der Diagramme für die Anzeige der zu erwartenden Datendurchsätze wählen. Wählen Sie die Option „Dynamische Skalierung“, wenn sich die Skalierung der Diagramme, wie zuvor beschrieben, automatisch in Abhängigkeit vom Datendurchsatz ändern soll.

Die dritte Schaltfläche für Ansichtsmodi zeigt den Datenverkehr als Pegelserie in horizontaler Ausrichtung, ohne Zeitachse, an. Die vierte Schaltfläche zeigt die gleichen Pegel, jedoch in vertikaler Ausrichtung (ohne Abbildung).

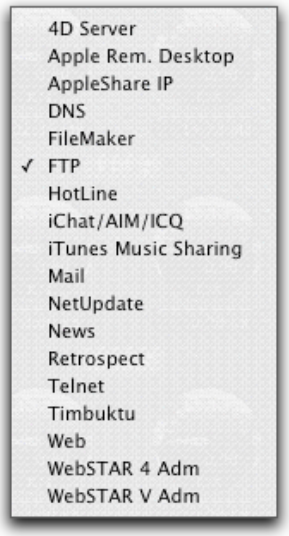
Die drei Ansichten, die runde Pegel enthalten, verfügen zudem über Schaltflächen zum Zurücksetzen. Wenn Sie auf diese Schaltfläche klicken, wird die untere Pegelzeile, die den gesamten Datenverkehr anzeigt, auf Null zurückgesetzt.

Auswählen der Arten von Netzwerkaktivitäten

In jedem Ansichtsmodus können Sie auswählen, welche Arten von Datenverkehr angezeigt werden sollen: Standardmäßig werden die Aktivitäten der Datentypen Web, FTP, Mail und iChat/AIM überwacht. Der fünfte Pegel zeigt jeden weiteren Datenverkehr an und der sechste das Gesamtdatenverkehrsaufkommen.

Sie können jedoch auch auswählen, welche Datentypen für die ersten vier Pegelpaare angezeigt werden sollen. Klicken Sie hierzu auf die Anzeige über einem der Pegel.

Nun können Sie den Typ der Netzwerkaktivitäten auswählen.



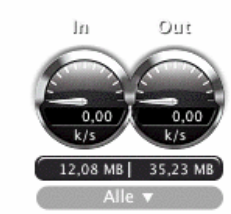
Über den Fensterabschnitt für Datenverkehrseinstellungen können Sie dieser Liste Dienste hinzufügen oder welche davon entfernen. Weitere Informationen erhalten Sie unter **Einstellungen für den Datenverkehr**.

NetBarrier-Monitor

Wenn Sie NetBarrier X5 installieren wird auch ein Programm namens NetBarrier-Monitor in Ihrem Programmordner platziert. Sie können dieses Programm starten, indem Sie auf das Programmsymbol doppelklicken. Oder Sie öffnen es über das Intego-Menü (siehe **Das Intego-Menü**).

NetBarrier-Monitor öffnet ein kleines, schwebendes Fenster, das es Ihnen ermöglicht, die Netzwerkaktivitäten ständig zu überwachen, ohne die Palette mit den Anzeigepegeln für die Netzwerkaktivitäten geöffnet halten zu müssen.

Nach dem Starten von NetBarrier-Monitor wird dessen Fenster mit den Anzeigepegeln in der unteren rechten Bildschirmecke angezeigt. Sie können diesen Ort ändern, indem Sie auf NetBarrier-Monitor klicken und das Fenster an eine andere Stelle auf Ihrem Bildschirm ziehen.



Standardmäßig zeigt NetBarrier-Monitor den gesamten Datenverkehr für alle Dienste an. Wie im Abschnitt für den Datenverkehr im Hauptprogramm von NetBarrier X5 können Sie ändern, welche Art von Datenverkehr angezeigt wird. Klicken Sie hierzu am unteren Rand des Fensters von NetBarrier-Monitor auf „Alle“ und wählen Sie einen Dienst aus dem Popup-Menü.

Wenn Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf eine beliebige Stelle im Fenster von NetBarrier-Monitor klicken, wird ein Popup-Menü mit zwei Optionen geöffnet.

Die Option „Im Dock anzeigen“ schließt das Fenster von NetBarrier-Monitor. Das Symbol von NetBarrier-Monitor im Dock ändert sich, um anzuzeigen, dass die Anzeigepegel in Echtzeit aktualisiert werden.

Die Netzwerkaktivität wird auch im NetBarrier-Monitor-Symbol angezeigt. Dieses Symbol wird eingeblendet, wenn Sie zwischen den Programmen wechseln, indem Sie auf Befehlstaste-Tabulator klicken.

Wenn wieder das Fenster von NetBarrier-Monitor geöffnet werden soll, müssen Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf das Symbol von NetBarrier-Monitor im Dock klicken und dann die Menüoption „Im Fenster anzeigen“ wählen.

Wenn NetBarrier-Monitor im Dock angezeigt wird, können Sie seine Anzeige ändern, wenn Sie bei gedrückter Steuerungstaste auf der Tastatur Ihres Macintosh auf das Symbol von NetBarrier-Monitor im Dock klicken und aus dem Dock-Menü einen anderen Dienst wählen.

Wenn Sie die Option „Im Dock behalten“ wählen, wird das NetBarrier-Monitor-Symbol dauerhaft im Dock abgelegt. Es bleibt auch dort, wenn das Programm nicht ausgeführt wird. Sie können es dann einfach öffnen, indem Sie auf das Symbol im Dock klicken. Wenn Sie die Option zum Öffnen beim Anmelden wählen, wird das Programm jedes Mal geöffnet, wenn Sie eine Benutzersitzung auf Ihrem Mac beginnen.

Einstellungen für NetBarrier-Monitor

Mehrere Optionen der Einstellungen haben eine Auswirkung auf das Verhalten von NetBarrier-Monitor. Sie können diese Einstellungen vornehmen, indem Sie „NetBarrier Monitor > Einstellungen“ wählen oder Befehlstaste-Komma drücken, während NetBarrier-Monitor ausgeführt wird.

Erscheinung	Anzeigepegel:  Thermometer:  Licht: 
Fensterniveau	Wenn Sie die Option „Über anderen Fenstern schweben“ wählen, wird NetBarrier-Monitor immer im Vordergrund angezeigt, über allen anderen Programmen.
Mausverhalten	Die Option „Mausklicks ignorieren“ sorgt dafür, dass Sie das Fenster von NetBarrier-Monitor nicht verschieben und die überwachten Dienste nicht ändern können.

Das Widget für NetBarrier-Monitor

Mit NetBarrier X5 wird ein Widget für NetBarrier-Monitor installiert, das in das Dashboard von Mac OS X (nur bei Mac OS X 10.4 Tiger oder neuer) geladen wird. In diesem Widget wird Ihnen jederzeit die Netzwerkaktivität angezeigt.

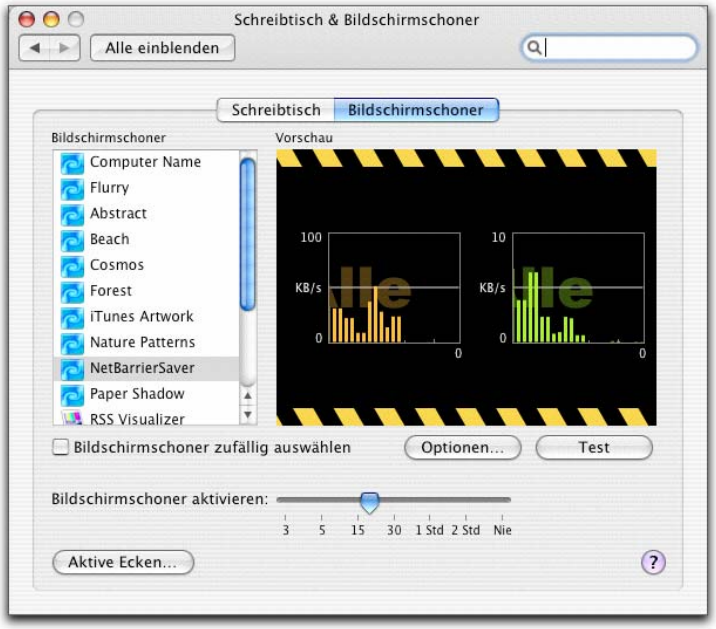
Aktivieren Sie das Dashboard, um sich das NetBarrier-Monitor-Widget anzeigen zu lassen. Klicken Sie auf die Schaltfläche „+“, wenn Sie sich alle auf Ihrem Computer verfügbaren Widgets anzeigen lassen möchten. Wählen Sie NetBarrier-Monitor aus der Liste. Das Symbol sieht folgendermaßen aus:

Durch Ihre Auswahl wird es zu den aktiven Widgets hinzugefügt. Sie sehen NetBarrier-Monitor immer, wenn Sie zum Dashboard wechseln. Wie beim Programm NetBarrier-Monitor können Sie das Fenster verschieben oder die Art der angezeigten Aktivitäten ändern.

Der Bildschirmschoner von NetBarrier X5

NetBarrier X5 installiert einen Bildschirmschoner, der Ihnen einen Überblick über die Netzwerkaktivitäten gibt, wenn Ihr Computer ansonsten nicht verwendet wird. Wenn Ihr Computer als Server betrieben wird, werden Sie durch diesen Bildschirmschoner zudem über die aktuellen Netzwerkaktivitäten informiert.

Wenn Sie den Bildschirmschoner von NetBarrier X5 verwenden wollen, müssen Sie die Menüoption „Systemeinstellungen…“ aus dem Apple-Menü wählen und dann erst auf die Schaltfläche „Schreibtisch & Bildschirmschoner“ und dann auf „Bildschirmschoner“ klicken. Wählen Sie „NetBarrierSaver“ aus der Liste der Bildschirmschoner.



Der Vorschaubildschirm zeigt nur den gesamten Datenverkehr an. Er zeigt jedoch den Datenverkehr nach einzelnen Diensten an, wenn diese tatsächlich ausgeführt werden. Klicken Sie auf „Optionen“ um festzulegen, in welcher Reihenfolge die Dienste angezeigt werden sollen.

Ziehen Sie die Dienste einfach in die gewünschte Reihenfolge. Die Anzahl der darstellbaren Dienste hängt von der Größe Ihres Bildschirms, der verwendeten Auflösung (Anzahl der Bildpunkte in beiden Achsen) und der Anzahl der verwendeten Videomonitore ab. Die wichtigsten sollten daher an erster Stelle stehen.

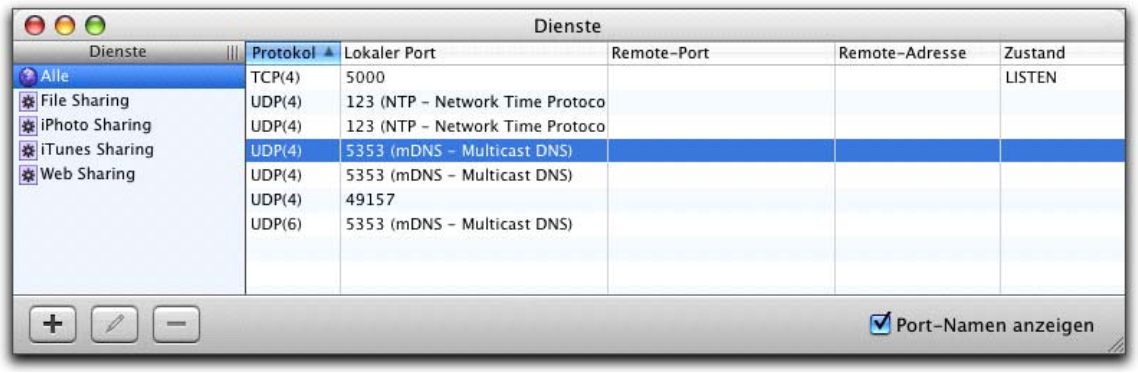
Weitere Informationen über die Einstellung von Bildschirmschonern finden Sie in der Hilfe zu Mac OS X.

Dienste

Das Dienstefenster zeigt alle aktiven Netzwerkdienste an, die auf Ihrem Computer für andere Benutzer über ein Internetprotokoll erreichbar sind, wie beispielsweise Webserver, Mailserver usw.

Klicken Sie auf das Symbol mit dem Doppelpfeil in der unteren rechten Ecke im Hauptfenster von NetBarrier X5, um sich das Dienstefenster anzeigen zu lassen.

Für jeden verwendeten Port werden die folgenden Informationen angezeigt: Das Protokoll (TCP oder UDP), die Nummer des lokalen Ports (abhängig vom jeweiligen Protokoll, wenn es ein Standardprotokoll ist, wie z.B. Port 21 für FTP), die Remote-Adresse (die IP-Adresse des anderen Computers) und der Status der Verbindung - beispielsweise ob die Verbindung aktiv ist oder nur Datenverkehr empfängt. Wenn Sie zusätzlich zu den Port-Nummern auch die Namen der Ports sehen möchten, klicken Sie auf das Kontrollkästchen „Port-Namen anzeigen“ in der unteren rechten Ecke, wie hier dargestellt.



Da die Liste der Ports, die von allen Diensten verwendet werden, sehr lang sein kann, bietet NetBarrier X5 Filter an, mit denen Sie sich die Ports anzeigen lassen können, die von bestimmten Diensten verwendet werden. Sie können zwischen File Sharing, iPhoto Sharing, iTunes Sharing und Web Sharing auswählen. Sie können aber auch eigene Filter erstellen.

Klicken Sie hierzu auf die Schaltfläche „+“ in der unteren linken Ecke des Fensters. Hierauf wird das Dialogfeld „Intelligenter Filter“ geöffnet.

Im ersten Popup-Menü können Sie festlegen, ob Sie möchten, dass der Filter mit einer der von Ihnen vorgegebenen Bedingungen übereinstimmt oder mit allen.

Das zweite Popup-Menü legt den Informationstyp fest, den der Filter suchen soll. Die Auswahl entspricht den Spalten im Dienstefenster: Protokoll, lokaler Port, Remote-Port, Remote-Adresse und Zustand. Nachdem Sie eine davon ausgewählt haben, können Sie die Filterdetails festlegen. In diesem Beispiel werden nur die Dienste aufgeführt, bei denen der lokale Port in einem bestimmten Rahmen liegt.

Wenn Sie auf das Pluszeichen in der rechten Fensterhälfte klicken, können Sie weitere Bedingungen hinzufügen. Wenn Sie hingegen auf das Minuszeichen neben einer Bedingung klicken, wird diese aus der Liste entfernt. Zudem können Sie Filterbedingungen auch verändern, indem Sie einfach die Option aus dem Popup-Menü ändern oder indem Sie neue Daten in das Datenfeld eingeben.

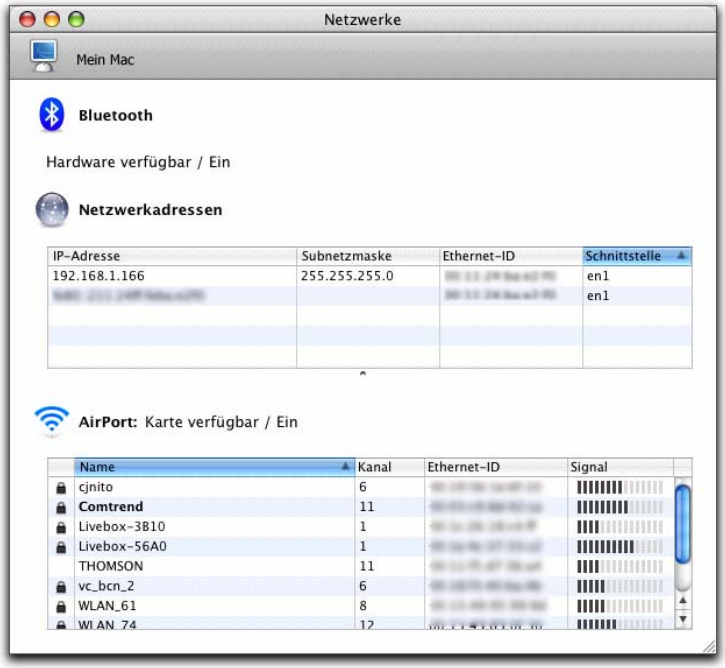
Wenn Sie Ihren Filter erstellt haben, klicken Sie zum Speichern auf „OK“. Geben Sie dann in der Diensteliste einen Namen für den Filter ein. Klicken Sie jederzeit auf den Filter in der Liste, um sich die Netzwerkdienste anzeigen zu lassen, die mit Ihren Bedingungen übereinstimmten.

Netzwerk

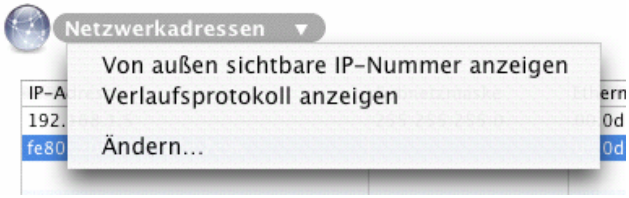
Das Netzwerkfenster zeigt hilfreiche Informationen über Ihren Mac an: die Netzwerkkonfiguration und die verfügbaren lokalen Netzwerke. Klicken Sie auf das Funkzeichen in der unteren rechten Ecke im Hauptfenster von NetBarrier X5, um sich das Netzwerkfenster anzeigen zu lassen.

Das Netzwerkfenster zeigt Folgendes an:

Name Ihres Mac	Wird in der grauen Leiste oben angezeigt: Im Beispiel unten ist das „Mein Mac“. Das ist der Name, den Ihr Computer jedem anzeigt, der danach in einem Netzwerk sucht. Sie können diesen Namen im Fensterabschnitt „Sharing“ der Systemeinstellungen ändern.
Bluetooth	Zeigt an, ob Bluetooth-Hardware verfügbar und aktiv ist.
Netzwerkadressen	Alle IP-Adressen, die auf Ihrem Mac aktiv sind. Wenn Sie mehrere Netzwerk-Adapter mit verschiedenen Adressen haben oder mehrere Server ausführen, wird mehr als eine Adresse angezeigt. Zeigt auch alle zugehörigen Subnetzmasken, Ethernet-IDs und Schnittstellen (im BSD-Namensformat) an.
AirPort	Verfügbarkeit und Status einer kabellosen Netzwerkkarte. Wenn Ihre AirPort-Karte verfügbar und eingeschaltet ist, zeigt die Tabelle verfügbare kabellose Netzwerke, ihre Kanäle, Ethernet-IDs und Signalstärken für Ihren aktuellen Standort an. (Je dunkler die Balken, umso stärker ist das Signal.) Für kabellose Netzwerke, die ein Passwort erfordern oder einen anderen Schlüssel, wird ein kleines Schlosssymbol angezeigt. Für Netzwerke ohne Schloss benötigen Sie kein Passwort zum Aufbau einer Netzwerkverbindung. Sie können jedoch auf andere Weise geschützt sein, wie z.B. durch eine Web-Authentifizierung. Wenn Sie mit einem kabellosen Netzwerk verbunden sind, wird der Name in Fettdruck angezeigt.



Wenn Sie auf „Netzwerkadressen“ klicken, stehen mehrere Funktionen und Optionen für das Netzwerkfenster zur Verfügung.

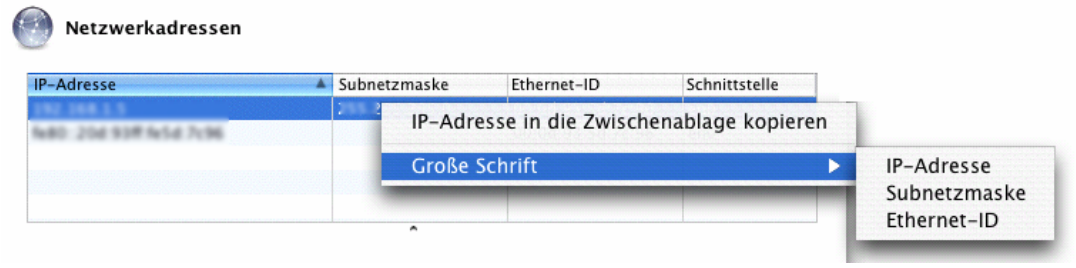


Zu diesen Optionen zählen:

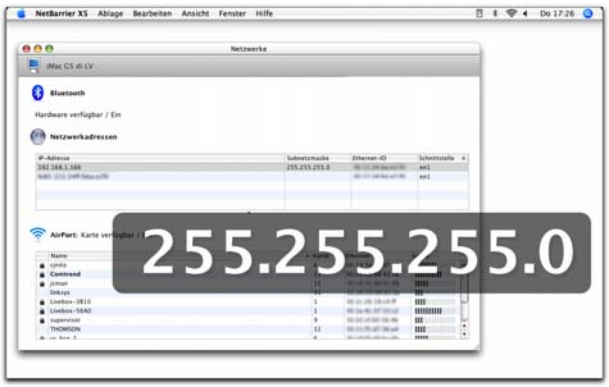
Von außen sichtbare IP-Nummer anzeigen	Diese Option zeigt in großer Schrift die IP-Adresse an, die Ihr Computer verwendet, wenn er mit dem Internet oder anderen Netzwerken verbunden wird. Diese IP-Nummer unterscheidet sich von der auf dieser Registerkarte angezeigten IP-Nummer, wenn Ihr Computer über einen Router oder ein Kabel oder ein DSL-Modem mit dem Internet verbunden ist. Klicken Sie auf eine beliebige Stelle auf dem Bildschirm, um die Information auszublenden.
Verlaufsprotokoll anzeigen	Zeigt eine Liste mit den verschiedenen IP-Adressen an, die Ihrem Mac in der Vergangenheit von Ihrem ISP zugewiesen wurden. Dies ist jedoch nur

	zutreffend, wenn Ihrem Mac keine feste IP-Nummer zugewiesen wurde. Wenn Ihr Computer über einen Router, ein Kabelmodem oder ein DSL-Modem mit dem Internet verbunden ist, wird lediglich die interne IP-Adresse Ihres Computers angezeigt.
Ändern...	Öffnet das Netwerkfenster in den Systemeinstellungen von Mac OS X. Sie können in diesem Fensterabschnitt den Namen oder die Netzwerkadresse Ihres Computers ändern. Weitere Informationen über die Netzwerkeinstellungen erhalten Sie in der Hilfe zu Mac OS X.

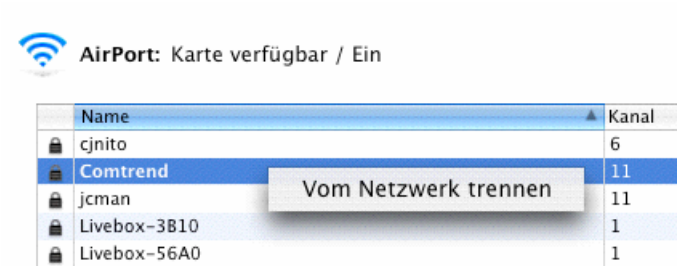
Weitere Optionen stehen auch für einzelne Einträge im Abschnitt für Netzwerkadressen zur Verfügung. Sie können sich diese anzeigen lassen, indem Sie die Steuerungstaste gedrückt halten, während Sie auf den gewünschten Eintrag klicken. Nun wird ein Kontextmenü geöffnet.



IP-Adresse in die Zwischenablage kopieren	Kopiert die Informationen im Nur-Text-Format in die Zwischenablage von Mac OS X. Von dort aus können Sie diese in andere Programme einfügen.
Große Schrift	Bietet die Möglichkeit, sich jede der drei Arten von Informationen für den Eintrag im Präsentationsmodus anzeigen zu lassen: die IP-Adresse, Subnetzmaske oder Ethernet-ID. Wenn Sie an eine beliebige Stelle auf dem Bildschirm klicken, wird die Anzeige in großer Schrift wieder ausgeblendet. Die folgende Abbildung zeigt ein Beispiel.



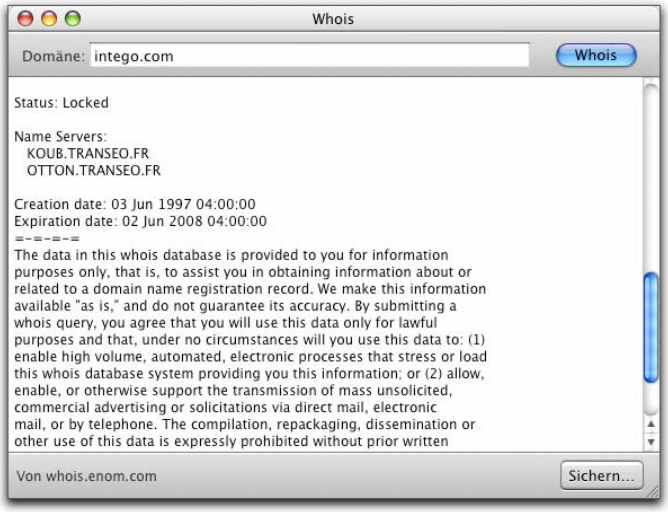
Wenn Sie schließlich mit der rechten Maustaste auf Einträge im AirPort-Abschnitt klicken, wird ein Kontextmenü geöffnet. Hier können Sie Ihren Mac von einem Netzwerk trennen, mit dem Sie derzeit verbunden sind.



Whois

In NetBarrier X5 können Sie Domänennamen und Internet-IP-Adressen überprüfen, indem Sie die integrierte Whois-Funktion verwenden. Diese Funktion können Sie starten, indem Sie auf das Fragezeichensymbol in der unteren rechten Ecke des Bildschirms klicken.

Geben Sie dann einen Domänennamen oder eine IP-Nummer ins Domänenfeld ein und klicken Sie auf die Schaltfläche „Whois…“ oder drücken Sie die Eingabetaste. Im Textfeld darunter sehen Sie nun die Informationen über die Domäne. Diese Informationen werden von öffentlich erreichbaren Informationsservern geliefert. Sie können diese Informationen in einer Textdatei sichern, indem Sie auf die Schaltfläche „Sichern...“ klicken.

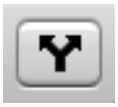


Nachdem Sie Ihre Informationen empfangen haben, zeigt der Text in dem grauen Balken am unteren Fensterrand Ihnen den Namen des Servers an, von dem die Informationen stammen. NetBarrier X5 enthält standardmäßig vier Whois-Server. Sie können diese jedoch ändern oder weitere Whois-Server angeben. Weitere Informationen über das Hinzufügen von Whois-Servern finden Sie im Kapitel 10, **Einstellungen und Konfigurationen**.

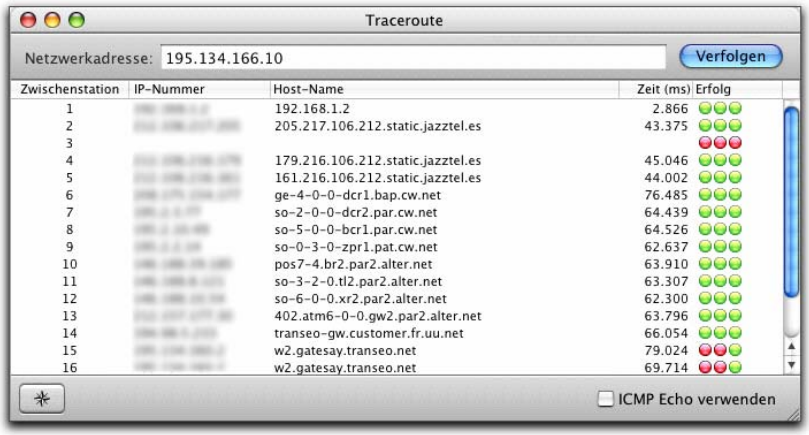
Traceroute

Wenn Sie Daten ins Internet oder ein anderes Netzwerk senden oder aus diesem empfangen, werden die Daten in Paketen von einem Host zum anderen gesendet, bis sie das Datenziel erreichen. Auf diesem Weg machen sie Dutzende von Sprüngen. Mit der Traceroute-Funktion von NetBarrier X5 können Sie genau verfolgen, wie Ihre Daten an ihr Ziel gelangen. Das ist vor allem dann hilfreich, wenn Sie Probleme haben, einen bestimmten Host zu erreichen und sehen möchten, wo die Daten blockiert werden. Wenn dies passiert bedeutet das normalerweise, dass ein Schlüssel-Host oder Router nicht funktioniert.

Starten Sie die Traceroute-Funktion von NetBarrier, indem Sie auf die Schaltfläche mit dem „Y-Pfeil“ in der unteren rechten Ecke des Bildschirms klicken.

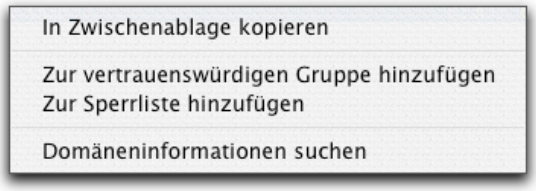


Sie können die Funktion „Traceroute“ verwenden, indem Sie eine IP-Adresse oder einen Domänennamen in das Feld „Netzwerkadresse“ eingeben und dann auf die Schaltfläche „Verfolgen“ klicken oder auf die Eingabetaste drücken. Wenn Sie einen Domänennamen eingeben, wird dieser von NetBarrier X5 in die entsprechende IP-Adresse aufgelöst, die dann angezeigt wird. Wenn Sie „ICMP Echo verwenden“ markiert haben, sendet Traceroute eine ICMP-Anfrage anstelle einer UDP-Anfrage. In einigen Fällen kann das effektiver sein.



Im Fenster „Traceroute“ werden nun alle Zwischenstationen (Relaisserver) zwischen Ihrem Computer und dem Zielserver angezeigt. Für jede Zwischenstation zeigt NetBarrier X5 die laufende Nummer, die IP-Adresse, den Domänennamen, die Reaktionszeit in Millisekunden und die Anzahl der Ping-Datentelegramme an, die erfolgreich (grüne Kreise) oder nicht erfolgreich (rote Kreise) übertragen wurden. NetBarrier X5 sendet für jede Zwischenstation oder jeden Schritt entlang der Route drei Pings. Wenn Ihr Computer über einen Router mit dem Internet verbunden ist, reagiert dieser unter Umständen nicht auf die Traceroute-Anfrage und zeigt möglicherweise eine fehlgeschlagene Anfrage an. Hierdurch wird die Verfolgung der Ping-Datentelegramme bis zum gewünschten Zielserver jedoch nicht unmöglich gemacht.

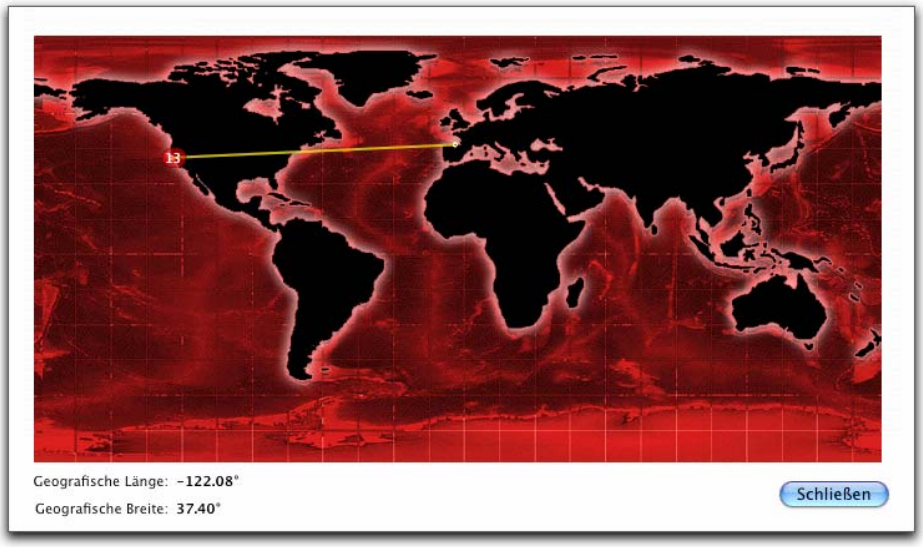
Wenn Ihre Traceroute-Anfrage abgeschlossen ist, können Sie mit der rechten Maustaste auf einen Eintrag klicken, um sich das Kontextmenü anzeigen zu lassen.



In Zwischenablage kopieren	Kopiert die Informationen im Nur-Text-Format in die Zwischenablage von Mac OS X. Von dort aus können Sie diese in andere Programme einfügen.
Zur vertrauenswürdigen Gruppe hinzufügen	Fügt diese IP-Adresse dauerhaft der Vertrauenswürdigen Gruppe hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen erlaubt. Die Firewall von NetBarrier X5 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-Adresse angewendet.
Zur Sperrliste hinzufügen	Fügt diese IP-Adresse dauerhaft der Sperrliste hinzu. So werden künftige Datenübertragungen von dieser Adresse ungeachtet der Antivandalismus-Einstellungen gesperrt. Die Firewall von NetBarrier X5 wird jedoch weiterhin auf die Datenübertragungen von dieser IP-Adresse angewendet.
Domäneninformationen suchen	Startet das Whois-Fenster von NetBarrier X5 und führt eine Suche nach der ausgewählten IP-Adresse durch. Weitere Informationen erhalten Sie unter **Whois**.

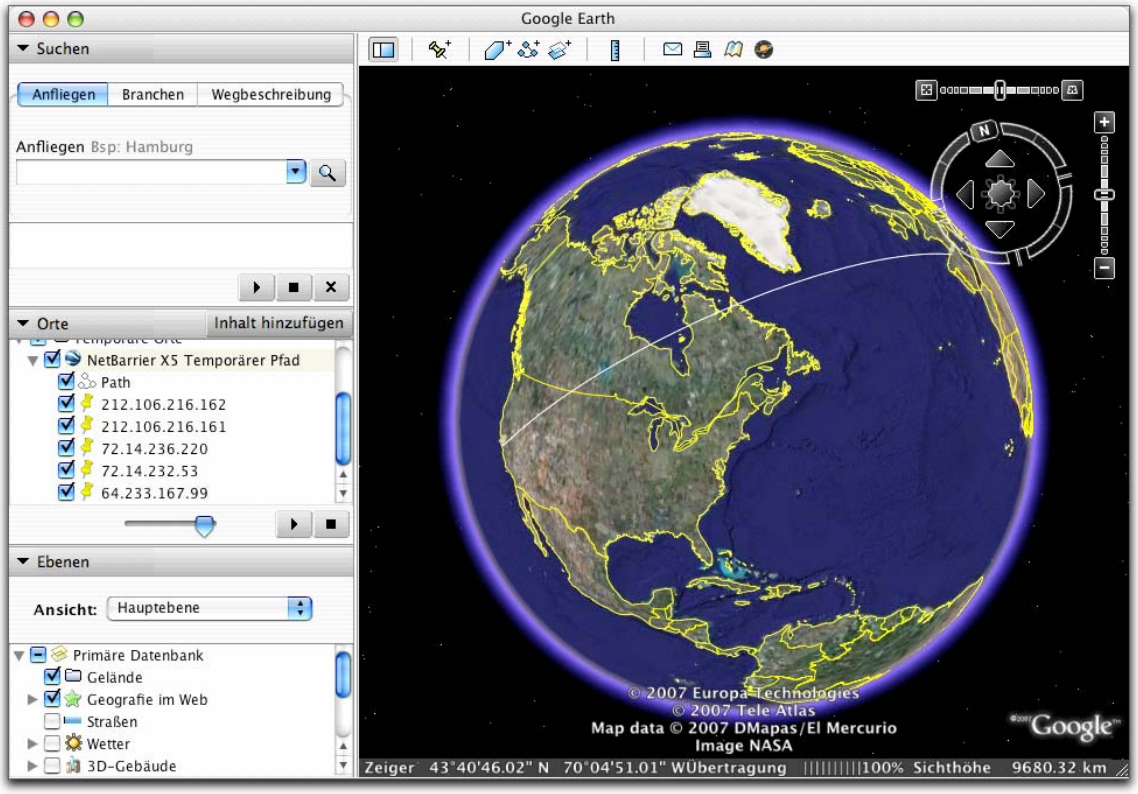
Sie können eine visuelle Anzeige der Route sehen, die Ihre Daten zurücklegt, indem Sie auf das Windrosensymbol in der unteren linken Ecke klicken.

Auf der Weltkarte sehen Sie nun Linien, mit denen der Zielserver über die Zwischenstationen mit Ihrem Computer verbunden ist. Hierbei werden die Nummern aller beteiligten Computer angezeigt.



Wenn Sie auf die Google Earth-Schaltfläche in der unteren linken Ecke klicken und die Software Google Earth auf Ihrem Mac installiert haben, öffnet NetBarrier X5 Google Earth und zoomt zu dem genauen geografischen Ort der IP-Adresse. Beachten Sie bitte, dass dies nicht für Adressen in Ihrem lokalen Netzwerk und auch nicht für alle IP-Adressen funktioniert.

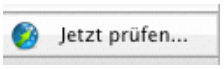
Der Pfad und die Zwischenstationen werden automatisch unter „NetBarrier X5 Temporärer Pfad“ im Abschnitt für Orte in Google Earth angezeigt. Weitere Informationen über das kostenlos herunterladbare Programm Google Earth finden Sie unter http://earth.google.com/intl/de/.


Google Earth
Suchen
Anfliegen
Branchen
Wegbeschreibung
Anfliegen Bsp: Hamburg
Orte
Inhalt hinzufügen
NetBarrier X5 Temporärer Pfad
Path
212.106.216.162
212.106.216.161
72.14.236.220
72.14.232.53
64.233.167.99
Ebenen
Ansicht:
Hauptebene
Primäre Datenbank
Gelände
Geografie im Web
Straßen
Wetter
3D-Gebäude
© 2007 Europa Technologies
© 2007 Tele Atlas
Map data © 2007 DMapas/El Mercurio
Image NASA
Google
Zeiger 43°40'46.02" N 70°04'51.01" W
Übertragung 100%
Sichthöhe 9680.32 km

NetUpdate

NetUpdate ist ein Programm für die automatische oder manuelle Aktualisierung der auf Ihrem Macintosh installierten Intego-Software. Das Programm NetUpdate wird gleichzeitig mit NetBarrier X5 oder einem anderen Anwendungsprogramm von Intego installiert. Intego NetUpdate prüft gleichzeitig alle auf Ihrem Computer installierten Intego-Programme auf die Verfügbarkeit neuer Versionen. Diese können dann von NetUpdate automatisch heruntergeladen und installiert werden.

NetUpdate sucht regelmäßig nach Aktualisierungen. Sie können das Programm auch sofort nach Aktualisierungen suchen lassen, indem Sie auf die Schaltfläche „Jetzt prüfen...“ in der oberen linken Ecke im Hauptfenster von NetBarrier X5 klicken.



Weitere Informationen über die Verwendung von NetUpdate finden Sie im Benutzerhandbuch von Intego für die ersten Schritte.

9 – Die Bedeutung von Warnmeldungen

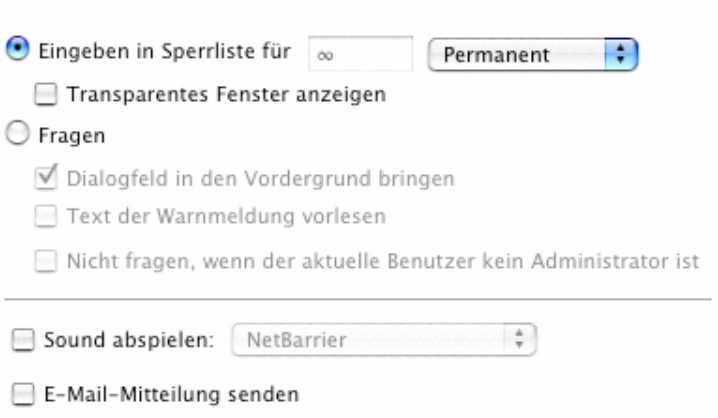
NetBarrier X5 überwacht die Netzwerkaktivitäten Ihres Computer zum Internet und zu lokalen Netzwerken dauerhaft und sucht nach bestimmten Datentypen, die auf einen Eindringversuch oder einen Angriff hinweisen. Wenn verdächtige Datenpakete gefunden werden, gibt NetBarrier X5 eine Warnmeldung aus, wobei Sie gleichzeitig gefragt werden, ob das Senden der Datenpakete erlaubt oder abgelehnt werden soll.

Einstellungen für die Warnhinweise

Warnhinweise werden als Reaktion auf die Einstellungen in den folgenden Bereichen angezeigt:

- Trojanische Pferde
- Daten
- Surfen
- Richtlinie
- Anti-Spyware

Einstellungen für diese Warnhinweise tauchen an mehreren Stellen in NetBarrier X5 auf, wie in den entsprechenden Abschnitten dieses Handbuchs beschrieben. Zur Erklärung dieser Einstellungen sehen wir uns an, wie sie im Abschnitt für Richtlinien auftauchen.



Eingeben in Sperrliste	Wenn dieses runde Optionsfeld markiert ist, werden die Verbindungen bei der Ausgabe einer Warnmeldung automatisch unterbrochen. Die IP-Adresse des angreifenden Computers wird sofort in die Sperrliste aufgenommen. (Siehe **Sperrliste und Vertrauenswürdige Gruppe**.) In einem Feld rechts vom runden Optionsfeld können Sie angeben, wie lang die IP-Adresse in der Sperrliste gespeichert werden soll. Sie können diese Zeitdauer in Sekunden, Minuten, Stunden oder Tagen angeben oder festlegen, dass die IP-Adresse des angreifenden Computers dauerhaft in die Sperrliste aufgenommen werden soll.
Fragen	Wenn dieses runde Optionsfeld markiert ist, zeigt NetBarrier X5 einen Warndialog an, indem Sie gefragt werden, was passieren soll. Wenn eine Warnmeldung erscheint, zeigt diese den standardmäßig gewählten Zeitraum der Sperrliste an. Dieser Zeitraum kann jedoch auf der Registerkarte für Richtlinien für jede Angriffsart geändert werden. Zudem haben Sie drei Optionen • **Dialogfeld in den Vordergrund bringen**: Die Warnmeldung wird bei einem Alarm automatisch in den Vordergrund gebracht. Andernfalls bleiben diese Fenster im Hintergrund (also hinter eventuellen anderen Fenstern auf dem Bildschirm Ihres Computers). Wenn Sie 90 Sekunden lang nicht auf eine Warnmeldung reagieren, wird das Fenster automatisch geschlossen. Die betreffende Verbindung mit Ihrem Computer wird abgelehnt. • **Text der Warnmeldung vorlesen**: NetBarrier X5 verwendet die Funktion „Text-to-Speech“ von Mac OS X, um den Text der Warnmeldung vorzulesen. • **Nicht fragen, wenn der aktuelle Benutzer kein Administrator ist**: NetBarrier X5 bietet die obigen Optionen nur an, wenn der Benutzer von Mac OS X über Administratorrechte verfügt. Andernfalls wird der angreifende Host automatisch in die Sperrliste aufgenommen.
Sound abspielen	NetBarrier X5 spielt bei jedem Alarm einen akustischen Warnhinweis Ihrer Wahl. Aus dem Popup-Menü rechts der Schaltfläche können Sie die gewünschte Klangdatei wählen.

E-Mail-Mitteilung senden	NetBarrier X5 sendet automatisch innerhalb von 30 Sekunden eine E-Mail-Mitteilung an die Adresse, die auf der Registerkarte „Optionen“ (siehe oben) konfiguriert wurde. (NetBarrier X5 wartet, ob noch andere Eindringversuche stattfinden, bevor die E-Mail-Mitteilung gesendet wird.)

Wenn Sie eine E-Mail-Benachrichtigung wünschen, müssen Sie Ihre E-Mail-Einstellungen so konfigurieren, dass Sie alle Warnmeldungen per E-Mail empfangen. Klicken Sie hierzu im Abschnitt für Richtlinien auf „Optionen“ und dann auf die Schaltfläche „Konfigurieren...“.

Sie müssen die E-Mail-Adressen für den Absender und den oder die Empfänger und den Namen des SMTP-Servers (für ausgehende E-Mail-Mitteilungen) eingegeben. Zudem müssen Sie einen Benutzernamen und ein Passwort eingeben, die Ihr Mailserver akzeptiert. E-Mail-Nachrichten können an mehrere Empfänger versendet werden. Klicken Sie auf die Schaltfläche „+“, um einen Empfänger hinzuzufügen. Klicken Sie auf die Schaltfläche „–“, um einen Empfänger zu löschen.

Beispiele für Warnhinweise

Das folgende Beispiel zeigt eine Warnmeldung, wenn das runde Optionsfeld „Eingeben in Sperrliste“ markiert und wenn das Kontrollkästchen „Transparentes Fenster anzeigen“ aktiviert ist.

Wie Sie sehen, haben Sie keine Wahlmöglichkeit, Sie erhalten nur eine Meldung. Wenn das Kontrollkästchen „Transparentes Fenster anzeigen“ nicht aktiviert wäre, würden Sie gar nichts sehen und NetBarrier X5 würde die IP-Adresse im Hintergrund der Sperrliste hinzufügen.

Das folgende Beispiel zeigt einen Warnhinweis, wenn das runde Optionsfeld „Fragen“ markiert und wenn das Kontrollkästchen „Dialogfeld in den Vordergrund bringen“ aktiviert ist.

In der oberen Zeile sehen Sie den Grund der Warnmeldung. Der Host (hier verschwommen) wird als IP-Adresse angezeigt. Sie können den zugewiesenen Domänennamen (sofern vorhanden) jedoch herausfinden, indem Sie auf das Fragezeichensymbol klicken. Wir haben bereits auf das kleine Dreieck geklickt, um weitere Informationen anzeigen zu lassen. Diese geben weitere Einzelheiten und Anweisungen an.

Durch Klicken auf eine der beiden Schaltflächen auf der unteren rechten Seite können Sie festlegen, was nun geschehen soll.

Sperrliste	In den meisten Fällen sollten Sie auf eine Warnmeldung durch Klicken auf die Schaltfläche „Sperrliste“ reagieren. Wenn Sie auf diese Schaltfläche klicken oder die Eingabetaste in der Tastatureinheit Ihres Computers drücken, wird der Empfang der Datenpakete von diesem Server gesperrt, sodass der Eindringversuch abgewehrt wird. Das empfangene Datenpaket wird nun ignoriert, als wäre es niemals empfangen worden. Wenn das empfangene Datenpaket Bestandteil einer Datei ist, so wird diese ebenfalls von Ihrem Computer ignoriert. Wenn das empfangene Datenpaket ein Befehl ist, wird er ebenfalls ignoriert und nicht ausgeführt. Zudem wird die IP-Nummer des Computers, der das Datenpaket an Ihren Computer gesandt hatte, automatisch in die Sperrliste aufgenommen und in dieser über die standardmäßig definierte Zeitdauer gespeichert. Diese Zeitdauer kann im Popup-Menü geändert werden.
Ignorieren	Wenn Sie auf diese Schaltfläche klicken, werden die Daten von Ihrem Computer gesendet. Der Datentransfer wird wie gewöhnlich fortgesetzt, bis NetBarrier X5 einen weiteren Eindringversuch erkennt. In diesem Fall wird ein weiterer Warnhinweis angezeigt.

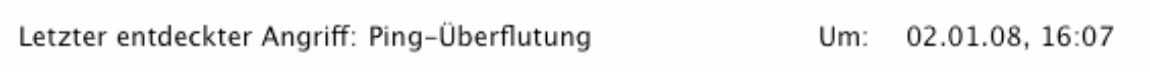
Schließlich zeigen wir noch ein Beispiel für eine Warnmeldung, die angezeigt wird, wenn ein Programm versucht hat, auf das Internet zuzugreifen und dabei eine Anti-Spyware-Regel verletzt hat.

Anti-Sypware-Warnungen verfügen über eine spezielle Funktion, durch die Sie sehen können, wo sich das angreifende Programm im Finder befindet. Klicken Sie auf den Namen des Programms (in diesem Beispiel „Firefox“). Dann können Sie das Programm sehen und zu dem Pfad navigieren.

Angriffszähler

NetBarrier X5 protokolliert die Anzahl der Angriffe, vor denen Ihr Computer geschützt wurde, und zeigt diese Anzahl in einem Zähler am oberen Rand des Bereichs für Richtlinien auf der Registerkarte „Antivandalismus“ an. Hier wird auch angezeigt, welche Art von Angriff zuletzt abgewehrt wurde, und wann dieser Angriff stattfand. Zuerst wird die Anzahl der Angriffe angezeigt:

Nach einigen Sekunden zeigt NetBarrier X5 Informationen über die letzten Angriffe an:



Sie können den Angriffszähler durch Klicken auf die daneben befindliche Schaltfläche „Zurücksetzen“ auf Null zurücksetzen.

10 – Einstellungen und Konfigurationen

Im Dialogfeld Einstellungen von NetBarrier X5 können Sie die Einstellungen für einige Funktionen von NetBarrier X5 ändern. Öffnen Sie dieses Fenster, indem Sie „NetBarrier X5 > Einstellungen...“ wählen oder Befehlstaste-Komma drücken. Daraufhin wird ein Fenster angezeigt, in dem das Modemsymbol ausgewählt ist, das erste von fünf Symbolen.

Einstellungen für das Modem

Diese Option ermöglicht es Ihnen, Ihren Modem so zu konfigurieren, dass er keine Anrufe annehmen kann. Klicken Sie hierzu im Dialogfeld „NetBarrier-Einstellungen“ auf die Schaltfläche „Modem“. Wenn Sie Ihr Modem sichern, kann es keine Anrufe mehr entgegennehmen. Wenn Sie auf die Schaltfläche „Jetzt schützen“ klicken, wird NetBarrier X5 keine eingehenden Anrufe akzeptieren: Sie können jedoch weiterhin ausgehende Anrufe tätigen. Durch Klicken auf die Schaltfläche „Zurücksetzen“ können Sie Ihr Modem wieder in den normalen, ungesicherten Zustand zurücksetzen.

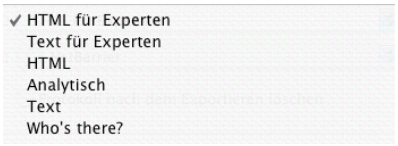
Protokolleinstellungen

Sie können NetBarrier X5 so konfigurieren, dass das Protokoll automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert wird. Klicken Sie hierzu im Fenster „NetBarrier-Einstellungen“ auf die Schaltfläche „Protokoll“.

Wählen Sie zuerst, wie oft das Protokoll exportiert werden soll. Wenn das runde Optionsfeld „Jede Woche“ markiert ist, wird das Protokoll immer um Mitternacht, von Sonntag auf Montag exportiert. Wenn „Jeden Tag“ markiert ist, wird es täglich um Mitternacht exportiert. Wenn „Jede Stunde“ markiert ist, wird es zu jeder vollen Stunde exportiert. Sie können auch eine benutzerdefinierte Option wählen und mehrere dieser Zeitpunkte eingeben, beispielsweise einmal alle zwei Wochen. (Mit der benutzerdefinierten Option können Sie das Protokoll auch einmal im Monat exportieren lassen, um Mitternacht des ersten Tages.)

Wenn der Computer zum Zeitpunkt des geplanten Exportvorgangs ausgeschaltet ist, wird das Protokoll dann exportiert, wenn Sie ihn das nächste Mal wieder einschalten.

Protokolle können in sechs verschiedenen Formaten exportiert werden. Klicken Sie ins Popup-Menü „Format“, um das Exportformat zu wählen.



Eine Beschreibung der Protokollexportformate erhalten Sie unter **So exportieren Sie das Protokoll**.

Sie können den Ordner wählen, in dem die Protokolldateien gespeichert werden sollen. Standardmäßig wird die Datei im Ordner /Library/Logs/NetBarrier gespeichert. Wenn diese Dateien in einem anderen Ordner gespeichert werden soll, müssen Sie auf die Schaltfläche „Andere...“ im Popup-Menü klicken und zum gewünschten Ordner navigieren. Klicken Sie dann auf die Schaltfläche „Wählen“, um diesen Ordner als Speicherort zu verwenden.

NetBarrier X5 verwendet zwei Protokolle. Es gibt ein Umlaufprotokoll, das höchstens 4096 Einträge enthält, die Ihnen im Protokollpaneel von NetBarrier X5 angezeigt werden. Wenn das automatische Exportieren aktiviert ist, werden alle Einträge in einem zweiten Protokoll gespeichert. Wenn Sie vollständige Protokolle aller Aktivitäten aufbewahren möchten, sollten Sie regelmäßige Exporte aktivieren. Diese Protokolle werden nicht durch die Größe begrenzt (außer durch den verfügbaren freien Speicherplatz auf Ihrer Festplatte). Wenn Sie die Option „Protokoll nach dem Exportieren löschen“ wählen, werden nach jedem Exportvorgang die Protokolleinträge gelöscht. So enthält jede neue Exportdatei nur die Einträge, die im Anschluss an den vorigen Export aufgezeichnet wurden. Diese Einstellung hat nur Auswirkungen auf automatisierte Exportvorgänge und nicht auf das manuelle Exportieren von Protokollen aus dem Protokollfenster.

Sie können auswählen, welche Elemente in Ihren Protokollen gespeichert werden sollen - wie durch die Kontrollkästchen am unteren Rand des Einstellungsfensters für Protokolle angezeigt. Sie haben folgende Optionen:

FrontEnd starten und beenden	Allgemeine NetBarrier X5-Aktivität, z.B. wenn NetBarrier X5 gestartet wird.
Abgelehnte Verbindungen	Versuche auf Ihren Mac zuzugreifen, die gesperrt wurden, weil von Ihnen in NetBarrier X5 eingestellte Regeln verletzt wurden.
Eingehende Daten werden durch die Sperrliste blockiert	Versuche von Hosts auf Ihrer Sperrliste Daten an Ihren Mac zu senden.
Ausgehende Daten werden durch die Sperrliste blockiert	Versuche von Ihrem Mac Daten an Hosts auf Ihrer Sperrliste zu senden.
Gesperrte Programme	Fälle in denen die Anti-Spyware von NetBarrier X5 dafür gesorgt hat, dass ein Programm keine Datenverbindung zu einem Netzwerk aufbaut.

Das letzte Kontrollkästchen lautet „Protokolle in Apples Log-Facility kopieren“. Wenn dieses markiert ist, werden die Protokolldaten in dem gemeinsamen Protokollsystem von Mac OS X 10.5 und neuer gespeichert.

Einstellungen für den Datenverkehr

Wie bei den Einstellungen für das Protokoll können Sie auch im Einstellungsfenster für den Datenverkehr zwischen verschiedenen Option für das Exportieren von Daten in regelmäßigen Zeitabständen wählen. Im nun geöffneten Fenster können Sie festlegen, wann und wie die Datenverkehrsdaten exportiert und verwaltet werden sollen. Klicken Sie zum Ändern der Einstellungen auf die Schaltfläche „Datenverkehr“ im Einstellungsfenster.

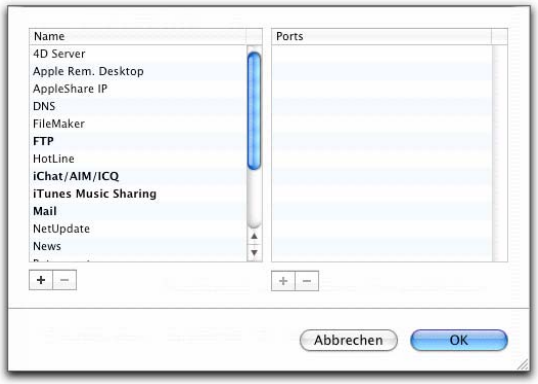
Im oberen Fensterabschnitt können Sie automatisierte, regelmäßige Exportvorgänge für den Datenverkehr festlegen. Das funktioniert genau so, wie bei den Einstellungen für das Protokoll: Weitere Informationen erhalten Sie im vorigen Abschnitt. Es gibt eine Einstellung, die sich von den vorherigen unterscheidet: das Kontrollkästchen „Anzeigepegel nach dem Exportieren zurücksetzen“. Dabei handelt es sich im Prinzip um die gleiche Funktion wie „Protokoll nach dem Exportieren löschen“. Wenn Sie das Kontrollkästchen markieren, passiert das Gleiche wie wenn Sie auf die Schaltfläche zum Zurücksetzen neben den Anzeigepegeln klicken, um den Gesamtdatenverkehr nach den automatisierten Exportvorgängen auf Null zurückzusetzen. Weitere Informationen über die Anzeigepegel für den Datenverkehr erhalten Sie unter **Verkehr**.

In den Einstellungen für den Datenverkehr von NetBarrier X5 gibt es eine Einstellung, mit der Sie das IP-Datenverkehrsaufkommen in ein- oder ausgehender Richtung überwachen können. Diese Funktion ist sehr nützlich, wenn das Datenverkehrsaufkommen (Datenvolumen, Datenmenge) Ihres Internet-Zugangs für gesendete und/oder empfangene Daten begrenzt ist.

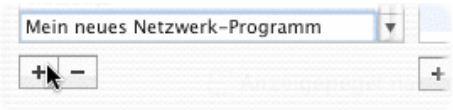
Wenn Sie diese Option markiert haben, gibt NetBarrier X5 eine Warnmeldung aus, sobald das Datenverkehrsaufkommen Ihres Computers den vorgegebenen Grenzwert überschritten hat. Sie können festlegen, ob die Alarmgabe bei ein- und/oder ausgehendem und/oder für den gesamten Datenverkehr erfolgen soll. Sie können den Grenzwert in Kilobyte, Megabyte oder Gigabyte angeben.

Darunter gibt es einen Abschnitt für die Erscheinungsweise. Hier können Sie die Farbe für den ein- und ausgehenden Datenverkehr in allen Anzeigepegeln und Zeitachsen für den Datenverkehr ändern. Wenn Sie auf eines der farbigen Kästchen klicken, wird die Standard-Farbauswahl von Mac OS X geöffnet: Wählen Sie die gewünschte Farbe aus und schließen Sie das Fenster dann, indem Sie auf das rote Schließsymbol in der oberen linken Ecke klicken. Wenn Sie auf die Schaltfläche „Auf Standardeinstellungen zurücksetzen“ klicken, wird der eingehenden Datenverkehr wieder orange und der ausgehende Datenverkehr grün angezeigt.

Schließlich gibt es noch eine Schaltfläche für Dienste im unteren Abschnitt, mit dem Sie die Art des in den Anzeigepegeln dargestellten Datenverkehrs verändern können. Diese Option ist sehr hilfreich, wenn Sie ein neues Netzwerkprogramm ausprobieren. Wenn Sie auf die Schaltfläche „Liste bearbeiten...“ klicken, wird ein Fenster geöffnet, in dem die vorhandenen Dienste aufgeführt sind.



Wenn Sie einen Dienst hinzufügen möchten, klicken Sie auf die Schaltfläche „+“ in der unteren linken Ecke des Fensters und geben Sie dann den Namen des Dienstes ein.



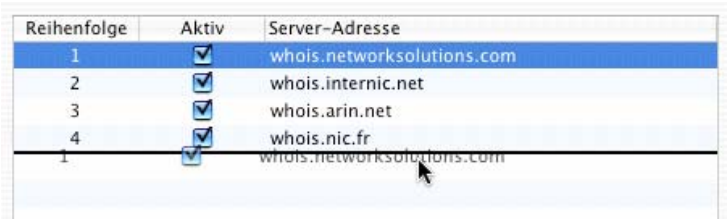
Wenn Sie dann auf das andere Pluszeichen unter der rechten Spalte klicken, solange der Dienst markiert ist, können Sie die zu diesem Programm zugehörigen Ports hinzufügen.

In ähnlicher Weise können Sie alle Dienste in der Liste bearbeiten oder löschen, die nicht in Fettdruck aufgeführt sind. Die fettgedruckten Dienste, wie beispielsweise Chat, Mai und Web, zählen zum Kern der Arbeit mit Netzwerken und sind daher aus Sicherheitsgründen für Veränderungen gesperrt.

Einstellungen für Whois

Die Whois-Funktion von NetBarrier X5 ermöglicht es Ihnen, den Domänennamen oder die IP-Adresse suchen zu lassen. In diesem Dialogfeld sind bereits vier Whois-Server vordefiniert, die in der angezeigten Reihenfolge abgefragt werden.

Sie können die Reihenfolge der Abfrage ändern, indem Sie auf den Domänennamen des betreffenden Whois-Servers klicken und diesen dann in die gewünschte Position ziehen.



Das Hinzufügen neuer Whois-Server zu NetBarrier X5 ist ganz einfach: Klicken Sie einfach auf das Pluszeichen und geben Sie den Namen des neuen Whois-Servers ein.

Sie können die Whois-Server in diesem Fenster auch aktivieren oder abschalten. Wenn Sie einen Server abschalten wollen, müssen Sie ins Kontrollkästchen links vom Namen des Filters klicken, sodass dort kein Häkchen erscheint. Um einen abgeschalteten Whois-Server wieder zu aktivieren, müssen Sie das entsprechende Kontrollkästchen markieren.

Wenn Sie einen Whois-Server entfernen möchten, klicken Sie zur Auswahl auf den entsprechenden Server und anschließend auf die Schaltfläche „–“. In einem Dialogfeld werden Sie dann gebeten, den Vorgang zu bestätigen.

Erweiterte Einstellungen

Im Fensterabschnitt „Erweitert“ in den Einstellungen für NetBarrier X5 stehen Ihnen drei Optionen zur Auswahl.

Konfiguration	Wenn Sie auf die Schaltfläche „Zur Standardeinstellung zurückkehren...“ klicken, wird NetBarrier X5 auf die Standard-Konfiguration zurückgesetzt: „Client, lokaler Server“-Modus für die Firewall und die Antivandalismus- sowie Datenschutzfunktionen sind deaktiviert. Um diese Konfiguration aktivieren zu können, benötigen Sie ein Administratorkennwort. Durch diesen Vorgang werden alle Ihre Firewall-Modi und alle anderen von Ihnen vorgenommenen Einstellungen ebenso wie Ihre Sperrliste und Ihre Vertrauenswürdige Gruppe gelöscht. Wir empfehlen Ihnen, Ihre aktuellen Einstellungen für NetBarrier X5 zu exportieren (Ablage > Einstellungen exportieren...), bevor Sie zu den Standardeinstellungen zurückkehren, falls Sie Ihre Einstellungen später erneut verwenden möchten.
Schutz	Wenn Sie auf die Schaltfläche „NetBarrier abschalten...“ klicken, wird NetBarrier X5 vollständig abgeschaltet – einschließlich der Protokollfunktion. Hierzu benötigen Sie ein Administratorkennwort. Sobald NetBarrier X5 abgeschaltet ist, wechselt die Schaltfläche auf „NetBarrier aktivieren…“. Wenn Sie NetBarrier wieder einschalten möchten, klicken Sie auf die Schaltfläche und geben Sie noch einmal ein Administratorkennwort ein. Ungeachtet dieser Einstellung wird NetBarrier X5 automatisch wieder aktiviert, wenn Sie Ihren Mac neu starten.

Konfigurations-assistent	Wenn Sie auf die Schaltfläche „Assistenten anzeigen…“ klicken, wird der Konfigurationsassistent von NetBarrier X5 gestartet. Weitere Informationen hierzu erhalten Sie in Kapitel 4, **Erste Schritte**.

Über NetBarrier X5

Wenn Sie die Option „Über NetBarrier…“ aus dem Menü von NetBarrier wählen, wird ein Fenster geöffnet, in dem Ihnen einige Informationen über NetBarrier X5 angezeigt werden - beispielsweise die Versionsnummer und Ihre Support-Nummer (eine Nummer, die Sie für die technische Kundenunterstützung benötigen).

Wenn Sie auf die Support-Nummer klicken, wird Ihr E-Mail-Programm mit einer an die technische Kundenunterstützung von Intego adressierten Nachricht geöffnet. In der Betreffzeile sind bereits Informationen angegeben, die es dem Support-Team von Intego erleichtern, auf Ihr Problem zu reagieren.

Konfigurationen

In NetBarrier X5 können Sie mehrere Konfigurationssätze speichern. Jeder Konfigurationssatz besteht aus allen Einstellungen von NetBarrier X5. Sie können Konfigurationssätze für verschiedene Orte definieren. Beispielsweise einen Satz dafür, wenn Sie Ihr Laptop im Büro verwenden und einen anderen dafür, wenn Sie es zuhause verwenden. Unter Umständen wollen Sie einen Konfigurationssatz mit zusätzlichem Schutz verwenden, wenn Sie Ihren Mac als Server einsetzen, während ein anderer Konfigurationssatz verwendet wird, wenn Ihr Mac nur als Client arbeitet. Sie können beispielsweise auch einen eigenen Konfigurationssatz speichern, den Sie verwenden, wenn Ihr Computer nur in ein Netzwerk integriert, aber nicht mit dem Internet verbunden ist. Ein anderer Konfigurationssatz bietet zusätzlichen Schutz, wenn Sie mit Ihrem Computer im World Wide Web surfen. Es kann auch zweckmäßig sein, einen Konfigurationssatz zu definieren und zu speichern, in dem Sie festgelegt haben, dass Intego NetBarrier X5 Ihnen eine E-Mail-Mitteilung schicken soll, sobald ein Eindringversuch erkannt wurde, wenn Sie nicht in der Nähe Ihres Computers sind.

Konfigurationen werden in einer Liste in der linken Hälfte des Hauptfensters angezeigt. (Weitere Informationen über das Hauptfenster erhalten Sie in Kapitel 4, **Erste Schritte**.) Mit den vier Schaltflächen unterhalb der Liste können Sie die Konfigurationen duplizieren, bearbeiten, entfernen oder ausblenden. Wenn die Konfigurationsliste nicht angezeigt wird, ist sie vielleicht ausgeblendet: Blenden Sie die Liste ein, indem Sie auf Befehlstaste-K drücken, „Ansicht > Konfigurationsliste ein-/ausblenden“ wählen oder auf die Schaltfläche ganz rechts klicken.

Erstellen, Bearbeiten und Löschen von Konfigurationen

Wenn Sie NetBarrier X5 zum ersten Mal verwenden, wird Ihnen eine Konfiguration namens „Standard“ in der Liste angezeigt. Wenn Sie eine neue Konfiguration erstellen möchten, können Sie den vorhandenen Satz duplizieren, indem Sie ihn markieren und dann auf die Schaltfläche ganz links klicken (sieht aus wie zwei Fenster). Sie können auch die Steuerungstaste drücken, dann auf eine vorhandene Konfiguration klicken und „Duplizieren“ aus dem Kontextmenü wählen. Geben Sie der neuen Konfiguration dann einen neuen Namen, indem Sie darauf doppelklicken und einen neuen Namen eingeben.

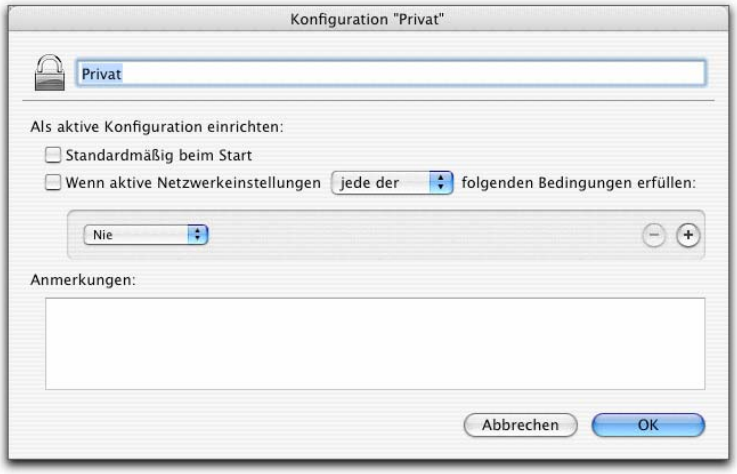
Jetzt können Sie den neuen Konfigurationssatz aktivieren, indem Sie auf das zugehörige runde Optionsfeld klicken. In unserem Beispiel haben wir zwei neue Konfigurationen erstellt, indem wir die Standard-Konfiguration zwei Mal dupliziert haben. Dann haben wir sie umbenannt und die ausgewählt, die jetzt „Privat“ heißt.

Anschließend können Sie die Konfiguration von NetBarrier X5 beliebig verändern und als aktuellen Konfigurationssatz speichern. Wenn Sie einen anderen Satz aktivieren möchten, klicken Sie einfach auf das entsprechende runde Optionsfeld. Sie können auch einen anderen Konfigurationssatz aus der Konfigurationsliste im Intego-Menü wählen.

Wenn Sie eine Konfiguration erstellt haben, gibt es drei Möglichkeiten, diese zu bearbeiten. Klicken Sie zuerst auf die Konfiguration. Dann haben Sie folgende Möglichkeiten:

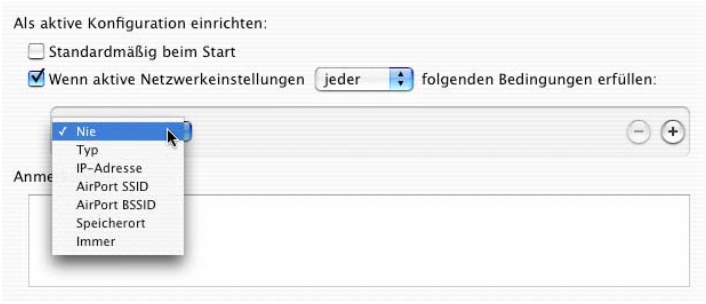
- Klicken Sie auf das Bleistiftsymbol am unteren Rand der Konfigurationsliste.
- Drücken Sie auf die Steuerungstaste während Sie auf die Konfiguration klicken und wählen Sie dann „Bearbeiten...“ aus dem Kontextmenü.
- Wählen Sie „Ablage > Konfiguration bearbeiten...“.

Ihnen wird dann ein Fenster angezeigt, dass so ähnlich aussieht, wie das folgende:



Diese Konfiguration wird aktiviert, wenn Sie Ihren Mac einschalten oder neu starten, wenn Sie das Kontrollkästchen „Standardmäßig beim Start“ markiert haben.

Zudem wird die Konfiguration automatisch aktiviert, wenn Sie das Kontrollkästchen „Wenn aktive Netzwerkeinstellungen...“ markieren und wenn eine oder alle von Ihnen für die folgenden Netzwerkkriterien festgelegten Bedingungen eintreten.



Nie	Diese Bedingung tritt nie ein, daher wird die Konfiguration auch niemals automatisch eingeschaltet.
Typ	Sie können wählen zwischen Ethernet, AirPort, FireWire, PPP oder Bluetooth.
IP-Adresse	Sie können eine bestimmte IP-Adresse wählen oder einen Bereich. Die Schaltfläche „Aktuell“ zeigt an, welche IP-Adresse Ihr Mac gerade verwendet.
AirPort SSID	Der übliche Name für ein kabelloses Netzwerk, z.B. „Mein AirPort“. Sie können auswählen, dass diese Bedingung eintreten soll, wenn die SSID entweder mit einer von Ihnen festgelegten Zeichenfolge übereinstimmt, nicht übereinstimmt oder Teile davon enthält.
AirPort BSSID	Die MAC-Adresse eines kabellosen Netzwerk-Verbindungspunkts. Sie wird als Zeichenfolge in Hexadezimal-Ziffern angegeben.
Umgebung	Der in den Netzwerkeinstellungen Ihres Mac festgelegte Speicherort.
Immer	Die Bedingung trifft immer zu.

Im Anmerkungsfeld können Sie eine Beschreibung oder Notizen in beliebiger Form eingeben, die Sie hinzufügen möchten. Sie haben keinerlei Auswirkungen auf die Funktionsweise der Konfiguration.

Sie können die Konfiguration auf zwei Arten löschen: Klicken Sie auf das Minuszeichen unter der Konfigurationsliste oder drücken Sie auf die Steuerungstaste während Sie auf die Konfiguration klicken und wählen Sie „Entfernen...“ aus dem Kontextmenü. In beiden Fällen wird daraufhin ein

Dialogfeld angezeigt, in dem Sie den Löschvorgang bestätigen müssen. Sie können die aktive Konfiguration nicht entfernen. Wechseln Sie stattdessen in eine andere Konfiguration, bevor Sie diese löschen.

Exportieren und Importieren von Einstellungen

Sie können Ihre Einstellungen von NetBarrier X5 in einer Datei speichern, aus der Sie die Einstellungen auf einem anderen Computer mit installiertem NetBarrier X5 importieren können. Dies ist vor allem dann zweckmäßig, wenn Sie mehrere Computer verwalten und für alle Computer die gleichen Einstellungen verwenden wollen.

Wählen Sie zum Exportieren der Einstellungen „Ablage > Einstellungen exportieren...“ aus. Daraufhin werden Sie in einem Dialogfeld aufgefordert, einen Namen für die Datei mit den Einstellungen einzugeben und einen Speicherort zu wählen. Klicken Sie auf „Exportieren“, wenn Sie fertig sind. Sie erhalten dann eine XML-Datei, die Sie in jede Kopie von NetBarrier X5 importieren können. Auch in die, in der die Datei erstellt wurde.

Wählen Sie hierzu die Option „Ablage > Einstellungen importieren…“. In einem Dialogfeld werden Sie aufgefordert, die Datei mit den Einstellungen zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf „Importieren“. Diese Einstellungen werden dann sofort auf NetBarrier X5 angewendet. Sie können auch auf die Einstellungsdatei von NetBarrier X5 doppelklicken, um sie zu importieren.

Sperren und Entsperren der Oberfläche

Die Bedienungselemente von NetBarrier X5 sind aufgrund der enormen Leistungsfähigkeit und Flexibilität des Programms sehr effektiv. Das Programm bemerkt jede festgestellte Netzwerkaktivität und reagiert auf sehr unterschiedliche Weise, je nachdem, welche Einstellungen Sie vorgenommen haben. Diese Leistungsfähigkeit kann auf der anderen Seite jedoch auch schwerwiegende Probleme verursachen, wenn die falschen Personen Zugriff auf das Programm erhalten. NetBarrier X5 gibt Ihnen daher die Möglichkeit, die Oberfläche des Programms zu sperren. So können auch diejenigen, die einen physikalischen Zugriff auf Ihren Mac haben, die Schutzfunktionen nicht verändern.

Sperren Sie NetBarrier X5 indem Sie entweder Befehlstaste-L drücken oder „Ablage > Oberfläche sperren“ wählen. Die Grundeinstellungen sind weiterhin sichtbar. Die Details können jedoch nicht berührt werden und niemand kann diese verändern, ohne zuvor die Oberfläche zu entsperren.

Wenn Sie NetBarrier X5 entsperren möchten, drücken Sie auf Befehlstaste-L oder wählen Sie „Ablage > Oberfläche entsperren“. Geben Sie dann Ihr Administratorpasswort ein, um den Vorgang abzuschließen.

11 – Technische Unterstützung

Als registrierter Intego-Kunde erhalten Sie von Intego technische Kundenunterstützung.

Per E-Mail:

eurosupport@intego.com: Europa, Naher Osten, Afrika

support@intego.com: Nord- und Südamerika

supportfr@intego.com: Frankreich

supportjp@intego.com: Japan

Über die Website von Intego

www.intego.com

Anerkennungen

Teile dieser Intego-Software können eventuell die folgenden Materialien verwenden, die durch Copyright geschützt sind. Die Verwendung derselben wird hierdurch anerkannt.

EDCommon und EDInternet Frameworks, geschrieben von Erik Dörnenburg.

Omni Development (OAGradientTableView)

12 – Glossar

Adressmaske	Eine Bitmaske zur Identifizierung, welche Bits in einer IP-Nummer mit der Netzwerkadresse und Subnetzelementen der Adresse übereinstimmen.
Adressmaskenabfrage	Ein Befehl zum Abfragen einer Adressmaske.
Adressmaskenantwort	Eine Antwort auf eine Adressmaskenabfrage.
ASIP	AppleShare-IP: Ein spezielles Protokoll für Apple-Netzwerkverbindungen.
Bootp	Das Bootstrap-Protokoll. Dieses Protokoll wird zum Starten von Arbeitsplatzcomputern verwendet, die über keine eigene Massenspeichereinheit verfügen.
Bootp-Client	Ein Computer, der als Bootp-Client arbeitet.
Bootp-Server	Ein Computer, der als Bootp-Server arbeitet.
Chat	Ein Dialogsystem, das es mehreren angemeldeten Teilnehmern ermöglicht, über ein Netzwerk zu kommunizieren, indem sie Informationen in ein Fenster tippen, die dann von den anderen Teilnehmern gesehen werden können. Die Aktualisierung dieser Informationen erfolgt häufig oder in Echtzeit.
Client	Ein Computersystem oder Prozess, das bzw. der einen Dienst von einem anderen Computersystem oder Prozess (einem Server) anfordert. Ein Arbeitsplatzcomputer, der eine Datei von einem Dateiserver anfordert, ist der Client dieses Servers.
Cookie	Eine kleine Datei, die ein Website-Server auf der Festplatte Ihres Computers speichert. Beim nächsten Besuch der gleichen Website wird das Cookie von Ihrem Webbrowser an eben diesen Website-Server zurückgesandt. Typischerweise werden Cookies dazu verwendet, um einen Benutzer wieder zu erkennen, nachdem er sich einmal bei einer Website angemeldet hat. Dadurch müssen die Anmeldeinformationen wie Benutzername und Passwort nicht mehr eingegeben werden. Cookies werden auch dazu verwendet, um den Einkauf im Internet zu vereinfachen. So können Sie zunächst Ware

	auf einer Website auswählen und in einen virtuellen „Einkaufswagen“ legen. Dank dem Cookie weiß der Website-Server später, welche Produkte oder Dienstleistungen Sie erwerben wollen, bevor es an die Bezahlung geht. Ein Cookie ermöglicht es auch, zu erkennen, welche Seiten einer Website Sie aufgerufen haben, sodass Ihnen auf Ihre persönlichen Vorlieben abgestimmte Seiten angeboten werden.
Datenpaket	Eine Dateneinheit, die über Netzwerke von einem Computer zu einem anderen übertragen wird. Ein Datenpaket enthält die Adresse des Absenders und des Empfängers, die Nutzdaten und andere Informationen.
Datentelegramm	Ein autonomes Datenpaket, das ausreichend viele Informationen enthält, um unabhängig von früheren und späteren Datentransfers von der Datenquelle zum Datenziel transportiert zu werden.
Dienst	Eine auf einem Server zur Verfügung stehende Netzwerkfunktion wie z.B. HTTP, FTP, E-Mail usw.
DNS	Domain Name System = Domänennamensystem. Ein von Routern im Internet verwendetes System zur Übersetzung von Domänennamen wie z.B. www.intego.com in die IP-Nummern (die eigentlichen Internet-Adressen) von Servern.
Echo	Eine während einer Ping-Aktion gesendete Abfrage.
Echoantwort	Die Antwort auf eine Echoabfrage.
Finger	Ein Programm zur Abfrage von Informationen über einen Benutzer im Internet oder einem anderen Netzwerk.
FTP	File Transfer Protocol = Dateitransferprotokoll. Ein Protokoll für die Übertragung von Dateien von einem Computer auf einen anderen. Für den Dateitransfer wird entweder ein Webbrowser oder ein spezielles FTP-Programm verwendet.
Gopher	Ein verteiltes Dokumentenabfragesystem (ein Vorläufer des World Wide Web).

Host	Eigentliche Bedeutung dieses englischen Begriffs: Gastgeber oder Wirt. In der Informationstechnologie ein mit einem Netzwerk verbundener Computer.
HTTP	HyperText Transfer Protocol = HyperText-Transferprotokoll. Dieses Protokoll ermöglicht die Übertragung von Website-Inhalten im World Wide Web.
ICMP	Internet Control Message Protocol = Internet-Protokoll für Status- und Kontrollmeldungen. Dieses Protokoll regelt die Aktionen von Fehler- und Kontrollmeldungen die während einer Datenübertragung von den beteiligten Computern ausgetauscht werden.
IGMP	Internet Group Management Protocol = Internet-Protokoll für die Gruppenunterstützung.
IMAP	Internet Message Access Protocol = Internet-Protokoll für den Zugriff auf Nachrichten. Dieses Protokoll ermöglicht einem Computer den Zugriff und die Verwaltung von E-Mail-Mitteilungen auf einem Mailserver. Die E-Mail-Mitteilungen können in Ordnern auf dem Mailserver verwaltet werden, wie dies mit E-Mail-Programmen auf einem Arbeitsplatzcomputer möglich ist.
Intranet-Datenwegelenkung	Die Auswahl der korrekten Schnittstelle und der nächsten Zwischenstation bei der Weiterleitung eines Datenpakets durch ein Intranet. Die Datenwegelenkung wird von einem Router übernommen.
IP	Internet Protocol = Internet-Protokoll. Die Netzwerkschicht des weit verbreiteten TCP/IP-Protokolls für die Datenübertragung in Ethernet-Netzwerken und im Internet.
IP-Nummer	Die Adresse eines Computers, der das Internet-Protokoll (IP) verwendet.
IRC	Internet Relay Chat = Internet-Relaisdialog. Ein Medium für die weltweite Echtzeitkommunikation vieler Teilnehmer übers Internet.

LAN	Local Area Network = lokales Netzwerk. Ein Netzwerk, über das mehrere Computer in einem örtlich begrenzten Bereich miteinander verbunden sind. Unter einem „örtlich begrenzten Bereich“ ist beispielsweise ein Gebäude, eine Werksgelände, ein Universitätsgelände oder Ähnliches zu verstehen.
NETBIOS	Network Basic Input/Output System = Basis-Eingabe- und -Ausgabesystem für Netzwerke. Eine Softwareschicht, die ursprünglich für die Verbindung eines Netzwerkbetriebssystems mit spezifischer Hardware vorgesehen war. NETBIOS kann auch die Kommunikation zwischen Arbeitsplatzcomputern in einem Netzwerk in der Transportschicht eröffnen.
Netzwerk	Eine Verbindung mehrerer Computer, die so miteinander verbunden sind, dass sie Daten untereinander austauschen können. Bei einem Netzwerk kann es sich um ein LAN oder um ein großes Netzwerk wie z.B. das Internet handeln.
NNTP	Network News Transfer Protocol = Netzwerknachrichten-Transferprotokoll. Ein Protokoll zum Verteilen, Abfragen, Abholen und Versenden von Diskussionsbeiträgen in Newsgroup übers Internet.
NTP	Network Time Protocol = Netzwerk-Zeitprotokoll. Dieses Protokoll stellt übers Internet die Synchronisation der in Computern eingebauten Echtzeituhren mit Funk-, Atom- oder anderen Uhren sicher. Dieses Protokoll ist in der Lage, geografisch verteilte Uhren langfristig mit einer Abweichung von nur wenigen Millisekunden zu synchronisieren.
Ping	Ein Programm zum Prüfen der Erreichbarkeit von Computern über ein Netzwerk. Das Programm sendet eine Echoabfrage und wartet auf eine Antwort.
Ping of Death	Ein besonders gefährlicher Ping-Angriff, der zum Absturz des empfangenden Computers führen kann.
Ping-Rundsenden	Ein Angriff ähnlich wie eine Ping-Überflutung. Siehe unten.

Ping-Überflutung	Ein Ping-Angriff auf einen Computer, wobei der Sender den Empfänger mit einer Flut von Echoabfragen überschwemmt. Dadurch wird der empfangende Computer überlastet und ist nicht mehr in der Lage, seine eigentlichen Tätigkeiten auszuüben.
POP3	Post Office Protocol (Postamtprotokoll), Version 3. POP3 ermöglicht es einem Client-Computer, E-Mail-Mitteilung von einem POP3-Server abzuholen.
Port-Scan	Das Abfragen der Ports eines Computers durch einen Eindringling, um herauszufinden, welche Dienste am angegriffenen Computer zur Verfügung stehen.
Protokoll	Ein Regelwerk für den Datenaustausch zwischen Computern in einem Netzwerk. Für den Datenaustausch im Internet stehen mehrere Protokolle (IP, HTTP, FTP, NNTP usw.) zur Verfügung.
Router	Eine Hardwareeinheit oder eine Software für die Weiterleitung von Datenpaketen zwischen Netzwerken, wobei der Router die Adressinformationen aus den Datenpaketen ausliest.
Rundsendepaket	In einem Ethernet-Netzwerk ist ein Rundsendepaket ein spezielles Datenpaket für den Empfang durch mehrere Datenziele, das von alle Knotenpunkten des Netzwerks empfangen wird.
Senden einer großen Anzahl von Verbindungs-anforderungen	Ein Angriff auf einen Computer, bei dem der sendende Computer den empfangenden Computer förmlich mit einer Flut von Datenpaketen überschwemmt, um Verbindungen mit ihm herzustellen. Dadurch wird der empfangende Computer überlastet und ist nicht mehr in der Lage, seine eigentlichen Tätigkeiten auszuüben.
Server	Ein Server (= Diener) ist ein Computer, der mit einem Netzwerk verbunden ist, und dessen Aufgabe darin besteht, anderen Computern im Netzwerk Daten oder Dateien zur Verfügung zu stellen. Diese anderen Computer werden als „Clients“ (= Kunden) bezeichnet.
SMTP	Simple Mail Transfer Protocol = einfaches

	Postübertragungsprotokoll. Ein Protokoll zum Übertragen von E-Mail-Mitteilungen zwischen Computern.
Spam	Unerwünschte E-Mail-Nachrichten, die Sie empfangen. Üblicherweise werden diese Mitteilungen zeitgleich an tausende oder millionen von Menschen geschickt, um Produkte oder Dienstleistungen zu verkaufen.
Spyware	Software, die heimlich Informationen von Ihrem Computer sammelt und diese an einen anderen Computer sendet.
TCP	Transmission Control Protocol = Sendesteuerungsprotokoll. Das meistverwendete Datentransferprotokoll in Ethernet-Netzwerken und im Internet.
TCP/IP	Die Internet-Version von TCP: TCP über IP.
Telnet	Das standardmäßige Internet-Protokoll fürs Anmelden bei entfernten Computern.
TFTP	Trivial File Transfer Protocol = triviales Dateitransferprotokoll. Ein einfaches Dateitransferprotokoll fürs Herunterladen des Urladeprogrammcodes auf Arbeitsplatzcomputer ohne eigene Massenspeichereinheit.
Traceroute	Ein Dienstprogramm zum Verfolgen von Datenpaketen auf ihrem Weg von einem Computer zu einem anderen.
Trojanisches Pferd	Ein schädliches Programm, das innerhalb eines Programms verborgen ist, das unschädlich zu sein scheint.
UDP	User Datagram Protocol = Benutzer-Datentelegramm-Protokoll. Ein Internet-Protokoll, das einfache, aber fehleranfällige Datentelegrammdienste zur Verfügung stellt.
Verbundene Dienste	Dienste, die eine bestehende Verbindung zwischen zwei Computern erfordern, also die Dienste HTTP, FTP, TELNET, SSH, POP3, AppleShare, usw. Dies betrifft alle TCP-Verbindungen.
Whois	Ein Internet-Verzeichnisdienst zum Suchen von Informationen über Domänennamen und IP-Nummern.