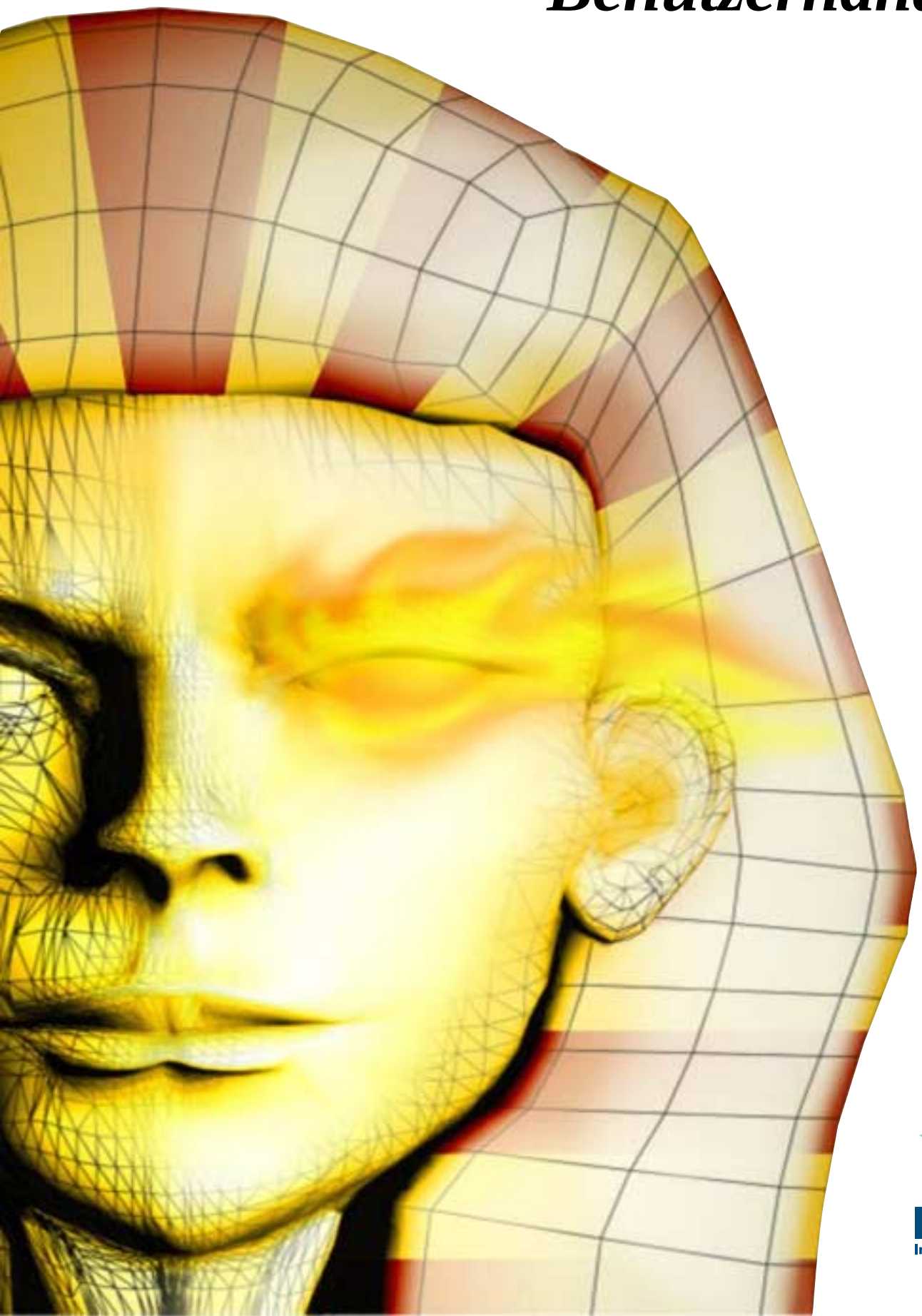
SPHINX PC Firewall

Benutzerhandbuch



Biodata
Information Technology

Inhaltsverzeichnis

1 Einführung 2

2 SPHINX starten 6

3 Sicherheit für PCs 8

4 Die SPHINX-Geheimnisse erkunden 15

4.1 Hauptkonsole 16

4.2 Pull-Down-Menüs 17

4.2.1 Datei 17

4.2.2 Konfiguration 18

4.3 Konsole Allgemeine Richtlinien 18

4.4 Internet-Kontrolle 20

4.5 Erweiterte Konfiguration 21

4.6 Konsole Protokollierung / Warnung 24

4.7 Konsole Administration 25

4.8 Protokollierungsüberwachungsprogramm 26

4.9 Warnungsüberwachungsprogramm 28

4.10 Statistikkonsole 29

1

Einführung

1 Einführung

SPHINX, die revolutionäre Personal Firewall, ist eine Firewall-Softwarelösung für den Schutz von einzelnen Desktop- und Notebook-PCs sowohl in Local Area Networks (LAN) als auch in Wide Area Networks (WAN). Dieses Tool von Biodata ist eine flexible Kombination von Sicherheitsmechanismen für ungeschützte Rechnerumgebungen. SPHINX schützt sowohl nicht vernetzte PCs von Privatanwendern als auch Computer in Unternehmensnetzwerken gegen Hackerangriffe.

Anwendern, die sich per Telefonleitung ins Internet einwählen bzw. die an kleine Netzwerke angeschlossen sind und nicht die Vorteile einer unternehmenseigenen Firewall genießen, bietet SPHINX ein leistungsfähiges und preiswertes Tool gegen Hackerangriffe, Trojaner und Scans. Zusätzlich können die Anwender alle Netzwerkzugriffe auf und von ihrem PC kontrollieren. Dazu kommt, dass eine Perimeter-Firewall keinen ausreichenden Schutz bietet, insbesondere nicht für die internen Anwendernetzwerke, die Angriffen schutzlos ausgeliefert sind, die von Rechnern innerhalb des Firewall-Bereichs ausgehen. SPHINX verhindert Hackerangriffe innerhalb des Netzwerks und sorgt dafür, dass zwischen den LAN-Rechnern die internen Zugriffsrichtlinien Anwendung finden.

SPHINX ist eine innovative PC-Firewall, mit der Sie Ihren Desktop-Computer (Windows 98/ Windows NT/Windows 2000) auf effiziente Weise vor Angriffen und Scans durch externe Nichtautorisierte schützen können. SPHINX kann auch die Kontrolle des Internet-Zugangs von Kindern, Schülern und Mitarbeitern übernehmen.

SPHINX verfügt über die folgenden Eigenschaften:

Sicher und leistungsfähig

SPHINX von Biodata arbeitet auf der untersten Stufe der Netzwerkhierarchie und kann dadurch das Betriebssystem und alle darüber liegenden Anwendungen vor allen Paketen schützen, die über die Netzwerkschnittstelle transportiert werden. Da das Programm im Kernel-Modus ausgeführt wird, bietet es die beste Leistung und den besten Schutz gegen Angriffe, auch gegen Angriffe gegen das Betriebssystem und seine Dienste. Im Gegensatz zu anderen Desktop-Firewalls, die sich auf den Schutz von Winsock-basierten Anwendungen beschränken, bietet SPHINX Netzwerksicherheit für alle Arten der PC-Kommunikation. SPHINX filtert alle Datenpakete, einschließlich IP-Protokolle (TCP, UDP, ICMP, NetBEUI usw.), indem es diese auf Geräteebene (Link Layer) erfasst. Auf diese Weise werden alle Pakete schon an der „Eingangspforte“ zum Netzwerk abgefangen.

Einfache Konfiguration und Anwendung

- Assistent: SPHINX enthält mehrere Assistenten zur intelligenten Konfiguration bis zur Expertenanwenderebene.
- Automatischer Lernmodus: SPHINX ermöglicht die Erstellung von Regeln in einem einzigen Durchgang. Im automatischen Lernmodus erläutert SPHINX den Inhalt jeder Kommunikation sowie die Risiken, die bestehen, wenn das Paket durchgelassen wird, so dass Benutzer mit geringen Vorkenntnissen von dem einfachen und umfassenden Regel-Lernmodus voll profitieren und auf einfache Weise Filterregeln erstellen können. Weiterhin werden innovative Lernmethoden angeboten (interaktiver oder Überwachungsmodus/explorativer oder Warnmodus), wodurch die Benutzer den jeweils anwenderfreundlicheren und einfacheren Modus auswählen können. Die wesentlichen Prinzipien der Kommunikation und der Auflösung der IP-Adressen werden ebenfalls dargestellt, um den Datenfluss zu veranschaulichen.
- Das Prinzip der Warnungsüberwachung kann diesen Lernmodus für die Benutzer weniger aufwendig machen, indem die Überprüfung von Sites nach und nach und mit anschließender Entscheidung über den Zugriff erfolgt (Möglichkeit der Einführung einer zeitlich begrenzten Testphase).

- Im explorativen Modus kann der Benutzer den Inhalt der Sites überprüfen und so leicht entscheiden, welche Kontrollmechanismen auf sie anzuwenden sind.
- Kontrolle über Internet-Dienste: das ursprüngliche Konzept der weißen und schwarzen URL-Listen. SPHINX ermöglicht die Angabe von Kontrollrichtlinien für jeden der verwendeten Internet-Dienste (Web, Chat, News, Telnet, FTP usw.). Die angegebenen URLs werden entweder gesperrt (schwarze Listen), oder der Zugriff darauf wird ausdrücklich gewährt (Konzept der weißen Liste). Listen mit Sites, auf die der Zugriff nicht gestattet werden soll, können auf einfache Weise aus vordefinierten URL-Listen importiert werden.

Umfangreiche Protokollierungs- und Warnfunktionen

- Intelligente Protokollierung: SPHINX ermöglicht die effiziente, durchgehende und detailgenaue Protokollierung des gesamten am PC ein- und ausgehenden Datenverkehrs. Eine Reihe von Protokollierungsfunktionen ermöglicht das Sortieren und Filtern von Protokollen sowie die Umsetzung von IP-Adressen in relative URLs. Die Protokollaufzeichnungen werden strukturiert dargestellt, um eine leichte und schnelle Durchsicht zu ermöglichen.
- Remote-Protokollierung: Der Administrator kann festlegen, dass SPHINX die zentrale Remote-Protokollierung aktivieren soll. Dabei wird direkt am Zugang zum PC protokolliert, wodurch der Endanwender keine Möglichkeit hat, die Protokollierung zu umgehen (IP-Spoofing).
- Leistungsfähige und innovative Kontrollfunktionen: Statusuntersuchungen von Scans und Trojanerangriffen. SPHINX verwendet eine spezielle Statusüberwachungstechnologie, um festzustellen, ob der PC von einem externen Rechner im Internet oder im LAN angegriffen oder analysiert wird. Dadurch kann jegliche Art von Hacker-Datenflüssen unterbunden werden, nicht nur TCP-basierte Angriffe. Externe IP-, UDP- und ARP-Kommunikation sowie nicht auf dem IP-Protkoll basierende Angriffe (IPX, NetBEUI usw.) werden ebenfalls verhindert. Für diese Verbindungsarten werden verschiedene Aktionen wie interaktive Warnungen und Überwachungswarnungen angeboten.
- Erweiterte Filtermöglichkeiten: Ein erweiterter Modus ermöglicht erfahrenen Benutzern, leistungsfähige Filterregeln für Nichtstandardprotokolle und -dienste selbst hinzuzufügen, zu ändern und zu löschen. Es können Regeln mit Zeitstempel mit der Möglichkeit der Erstellung von Protokollen und Warnungen angegeben werden.
- Zeitliche Zugangskontrolle: In SPHINX kann die Uhrzeit, das Datum und auch die Dauer von Netzwerkverbindungen genau angegeben werden. Dadurch können Benutzersitzungen sehr genau kontrolliert werden.
- Sicherheitsprofile für mehrere Benutzer: In SPHINX können für jeden einzelnen Benutzer die geeigneten Sicherheitszugangsrichtlinien festgelegt werden.
- Sicherheitsrichtlinien für mehrere Geräte: In SPHINX können für jedes einzelne Gerät vollständige Sicherheitszugangsrichtlinien festgelegt werden.
- Versteckter Kontrollmodus: Das SPHINX-Programmsymbol und die Verknüpfung mit SPHINX kann für den PC-Benutzer unsichtbar gemacht werden, damit er von der Existenz von und der Kontrolle durch SPHINX keine Kenntnis erlangt.
- Anwendungs- und Dienstetransparenz: SPHINX von Biodata wird im Hintergrund ausgeführt und wird dadurch für den Endbenutzer nicht unmittelbar sichtbar. SPHINX arbeitet nahtlos und sicher mit anderen Anwendungen zusammen.

Installation von SPHINX

Systemanforderungen

Um SPHINX verwenden zu können, müssen folgende technische Anforderungen erfüllt sein

- mindestens Pentium-CPU
- Windows 98, Windows NT, Windows 2000
- mindestens 32 MB RAM
- 5 MB freier Speicherplatz auf der Festplatte
- CD-ROM-Laufwerk

Installationsablauf

Zur Installation von SPHINX müssen die folgenden Schritte durchgeführt werden:

- Den PC hochfahren
- Die SPHINX-CD-ROM einlegen
- Auf „Installieren“ klicken und den Anweisungen folgen
  (Falls das Startfenster nicht automatisch geöffnet wird, die Datei **setup.exe** auf der CD-ROM ausführen)
- Je nach verwendetem Medium (LAN, MODEM, ISDN) muss die Filter-Engine durch Klicken auf „Engine-Installationsprogramm“ installiert werden
- Den PC neu hochfahren

Achtung: Um Probleme zu vermeiden, ist es notwendig, vor dem Entfernen einer Netzwerkkarte oder eines Modems aus dem PC den SPHINX-Treiber zu entfernen.

2

SPHINX starten

2 SPHINX starten

Klicken Sie zum Start auf das SPHINX-Symbol. Sie können überprüfen, ob die Software erfolgreich installiert wurde, indem Sie auf der Hauptkonsole „Zugang für alle zulassen“ aktivieren.



SPHINX wird jetzt im transparenten Modus ausgeführt, und die Filter-Engine lässt alle Pakete ohne Prüfung passieren. Es müssen jetzt alle Dienste wie vor der Installation der Firewall-Software funktionieren. Wenn dies der Fall ist, aktivieren Sie anschließend „Zugang für alle sperren“.



Auf diese Weise kann eine Konfiguration eingerichtet werden, die ausschließlich die Dienste verwendet.

3

Sicherheit für PCs

3 Sicherheit für PCs

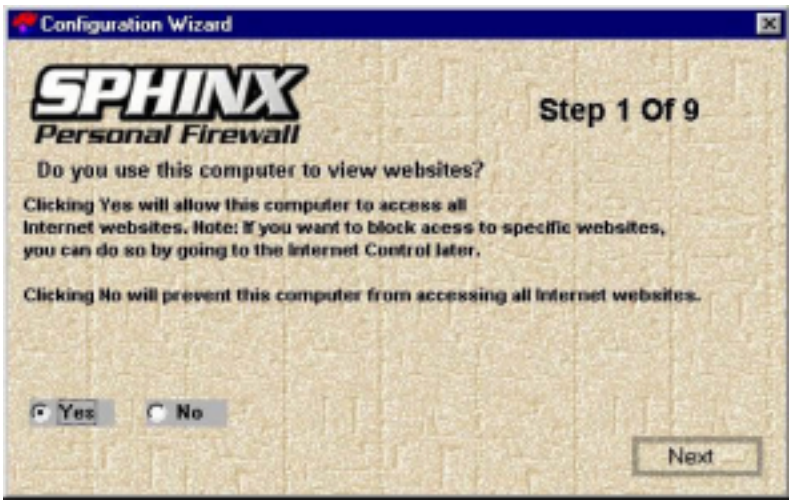
Normalerweise sollte der Schutz des Netzwerks gewährleistet sein, bevor das Netzwerk mit dem Internet verbunden wird. Dazu sollte eine Firewall installiert werden. Diese Firewall überprüft alle vom Internet kommenden Pakete und entscheidet je nach Konfiguration, ob die verschiedenen Pakete durchgelassen werden. Außerdem prüft die Firewall auch die vom internen Netzwerk ins Internet geschickten Pakete. Damit ist der Schutz der Rechner im internen Netzwerk gewährleistet.

Dieselbe Situation liegt bei PCs ohne Netzwerkanschluss vor, die mit dem Internet verbunden sind. Normalerweise können nicht alle ankommenden und abgehenden Datenströme eines PCs kontrolliert werden, so dass die Benutzer Angriffe auf ihren Rechner nicht erkennen können. Wenn jedoch ein „Trojaner“ auf ihrem PC installiert ist, haben Hacker Zugriff auf den Rechner und können mit Hilfe von Hacker-Tools wie Netbus und Sub7 jeden ungeschützten PC vollständig kontrollieren. Daher ist Firewall-Sicherheit nicht nur ein Thema für große Computernetzwerke, sondern auch für jeden eigenständigen PC.

Sicherheitsrichtlinien definieren die Aktionen, die dazu beitragen, ein Netzwerk oder einen PC sicher zu machen. Diese Sicherheitsrichtlinien enthalten auch die Liste der Dienste, die das Firewall-System zulassen soll. Eine Firewall-Konfiguration sollte immer so eng wie möglich gefasst sein, also nur die Dienste zulassen, die wirklich benötigt werden. SPHINX verfügt über Funktionen, mit denen die Sicherheitsrichtlinien für einen einzelnen PC umgesetzt werden können, auch für einen Administrator, der mit Sicherheitsproblemen im Internet nicht sehr vertraut ist. Die beste Wahl für Unerfahrene in diesem Bereich ist die Verwendung des Assistenten.

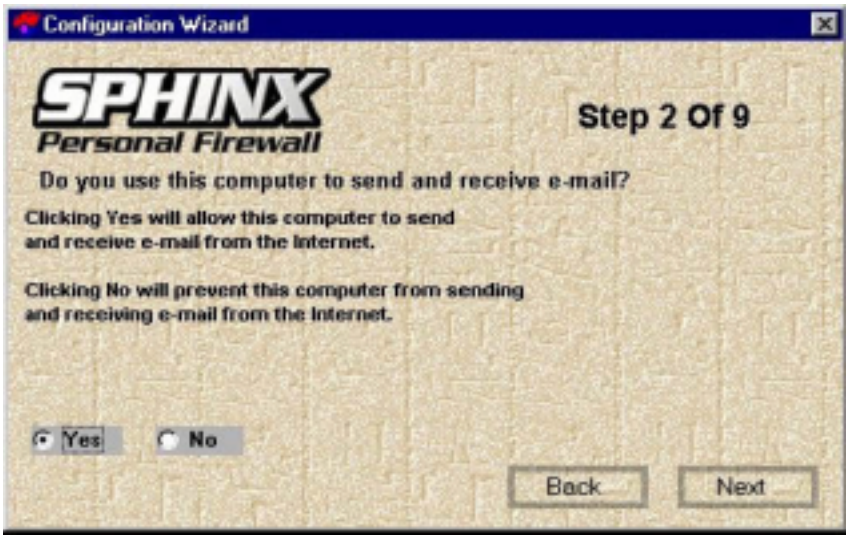
Der Konfigurationsassistent unterstützt Sie bei der Erstellung der ersten Konfiguration. Er fragt Schritt für Schritt, wie die speziellen Dienste zu konfigurieren sind. Der Anwender kann alle Fragen mit einem einfachen Ja oder Nein beantworten. Mit Hilfe des einfach zu bedienenden Konfigurationsassistenten kann eine effektive Firewall-Basiskonfiguration erstellt werden.

Schritt 1: Möchten Sie Web-Seiten anzeigen?



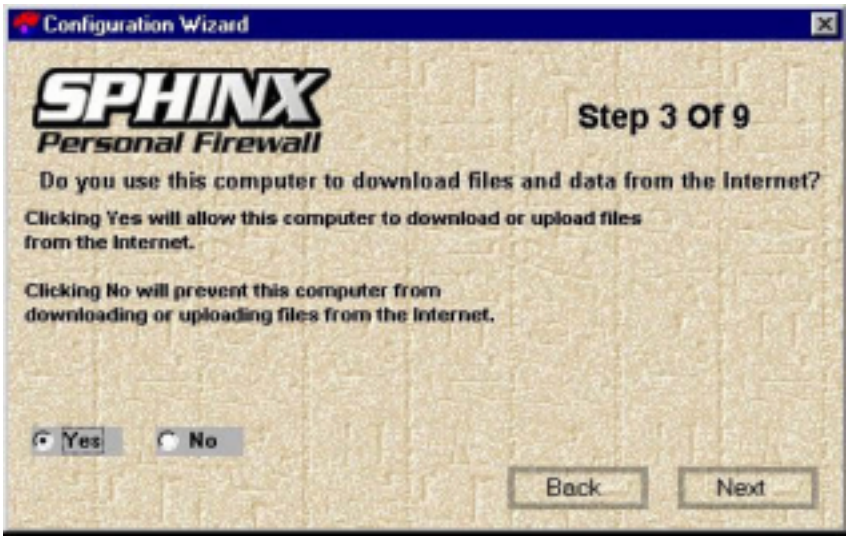
Wenn Sie mit „Ja“ antworten, lassen Sie damit den Zugriff auf alle Websites im Internet ohne Beschränkung zu. Wenn Ihr PC auch von Kindern benutzt wird und Sie den Internetzugang deshalb kontrollieren möchten, können Sie hier auf „Ja“ klicken und die Form der Kontrolle später in den Menüs „Erweitert“ und „Internet-Kontrolle“ (5.3, 5.4) angeben. Zum Beispiel: Sie können Listen erstellen, die Websites enthalten, für die der Zugang generell gesperrt sein soll (schwarze Listen). Sie können auch eine weiße Liste definieren, die alle Websites enthält, auf die zugegriffen werden darf. SPHINX sperrt dann den Zugang zu allen Websites, die nicht in der weißen Liste enthalten sind.

Schritt 2: Möchten Sie E-Mails senden und empfangen?



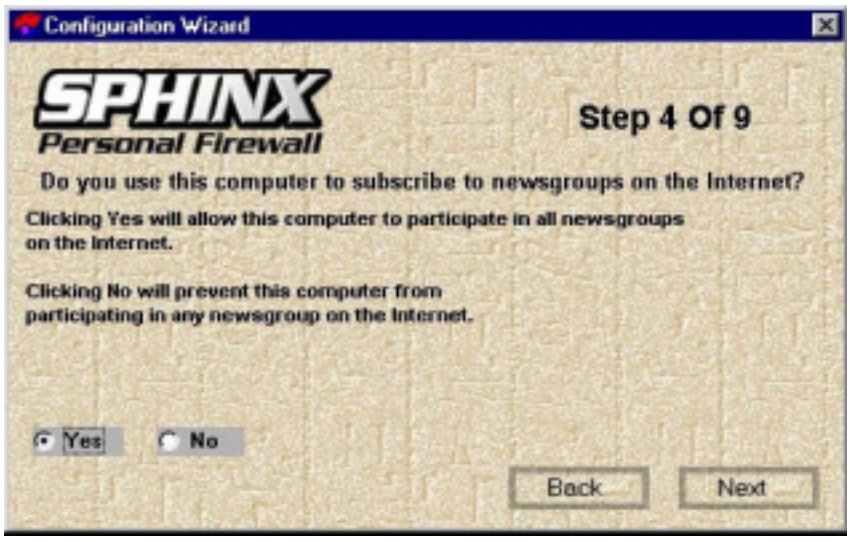
Wenn sie mit „Ja“ antworten, können Sie E-Mails über SMTP (Simple Mail Transport Protocol) senden und über POP3 empfangen. E-Mails können dann zu allen Servern im Internet geschickt und von dort empfangen werden. Diese elektronische Kommunikation ist wegen ihrer hohen Übertragungsgeschwindigkeit bei den Internetbenutzern sehr beliebt.

Schritt 3: Möchten Sie Dateien, Bilder und Daten aus dem Internet herunterladen?



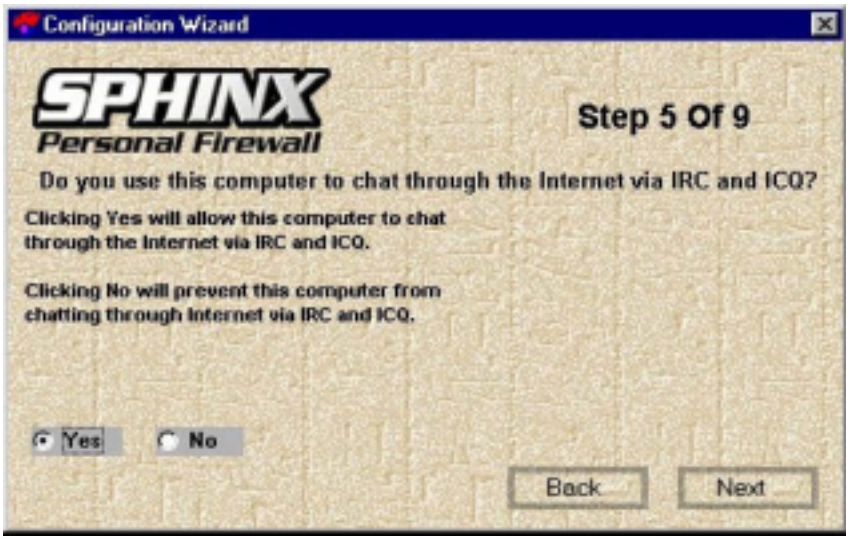
Wenn Sie auf „Ja“ klicken, können über Ihren PC alle Arten von Dateien, Bildern und Daten aus dem Internet heruntergeladen werden. Wenn Sie den Download von z.B. Website-Texten auf Ihren PC oder auf Diskette beabsichtigen, sollten Sie diese Option aktivieren. Das gleiche gilt für Bilder und komplette Programme wie Spiele, die oft kostenlos aus dem Internet heruntergeladen werden können.

Schritt 4: Möchten Sie sich an Newsgroups im Internet beteiligen?



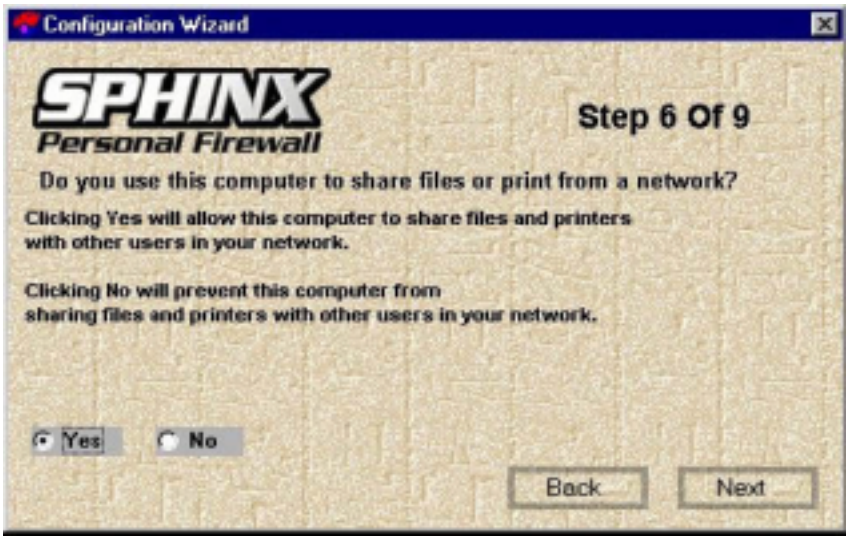
Newsgroups im Internet ermöglichen den Gedanken- und Erfahrungsaustausch zu verschiedenen Themen. Wenn Sie z.B. einen Rat zu einem speziellen Problem mit Ihrem Computer suchen, können Sie in Newsgroups die Lösung finden. Zum Lesen dieser Nachrichten bzw. zum Senden eigener Nachrichten benötigen Sie einen so genannten Newsreader. Der Web-Browser „Navigator“ von Netscape enthält einen Standard-Newsreader. Selbstverständlich sind auch andere Newsreaders verfügbar.

Schritt 5: Möchten Sie im Internet chatten?



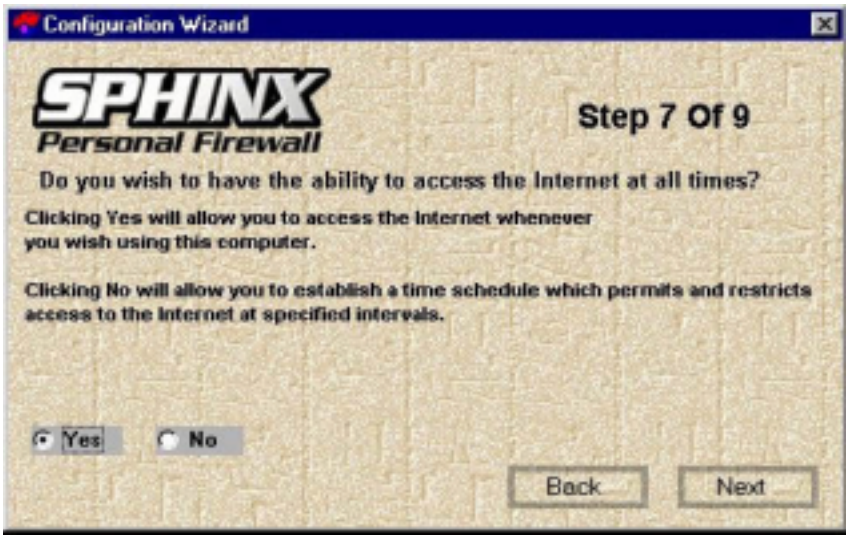
Beim Chatten können Sie gleichzeitig mit mehreren anderen PC-Benutzern über das Internet kommunizieren. Dazu müssen Sie sich zuerst bei einem geeigneten Server registrieren lassen, über den Sie dann Nachrichten austauschen können. Im Internet gibt es sehr viele Chatrooms zu den verschiedensten Themen, in denen Sie Ihre Meinung sagen können.

Schritt 6: Möchten Sie auf Dateien und Drucker gemeinsam mit anderen Benutzern im Netzwerk zugreifen?



Drucker, die an einen einzelnen PC im Netzwerk angeschlossen sind, können auch von anderen Benutzern im Netzwerk verwendet werden. Der Zugriff durch andere Benutzer muss in diesem Fall in der Netzwerkkonfiguration festgelegt werden. Wenn in Ihrem PC ein Modem oder eine ISDN-Karte installiert ist, d.h., wenn Ihr PC nicht über Ethernet an das Netzwerk angeschlossen ist, ist diese Funktion aller Wahrscheinlichkeit nicht erforderlich. In diesem Fall wird der Drucker oft direkt an den PC angeschlossen, damit Druckaufträge nicht über das Netzwerk geschickt werden.

Schritt 7: Möchten Sie unbegrenzten Zugang zum Internet haben?

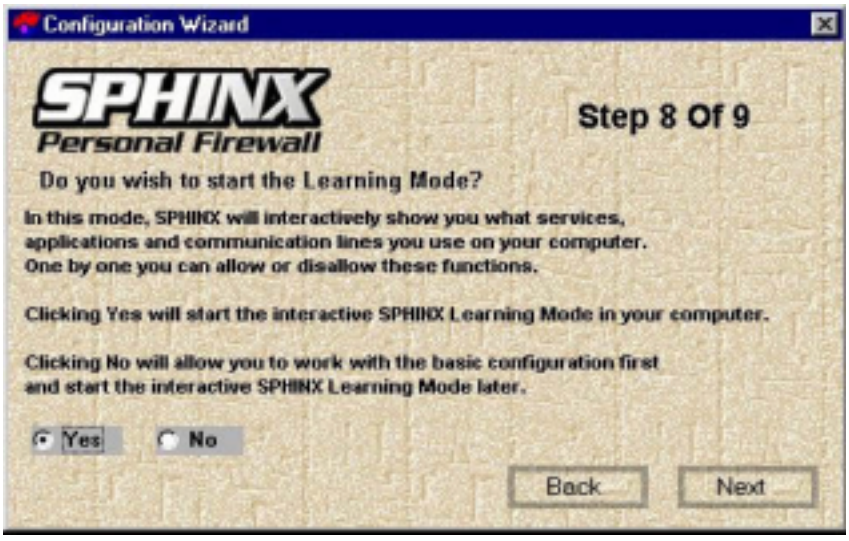


Wen Sie mit „Ja“ antworten, haben Sie ständig Zugang zum Internet. Das gilt nicht nur für Sie, sondern auch für andere PC-Benutzer, z.B. Kinder und Mitarbeiter. Wenn Sie auf „Nein“ klicken, können Sie den folgenden Zeitplan ausfüllen:



In den ersten zwei Feldern kann das Anfangs- und Enddatum für die folgenden Zeiteinstellungen festgelegt werden. Wenn Sie diese Zeiteinstellungen über das festgelegte Enddatum hinaus verwenden möchten, können Sie die Einstellungen einfach für die entsprechende Zeitspanne wiederholen. Mit SPHINX können Sie den Zugang zum Internet entweder auf eine bestimmte tägliche Gesamtzeit oder auf bestimmte Tage der Woche begrenzen. Bei der Einstellung der Zeit nach Zeitdauer wird der Zugang zum Internet auf eine bestimmte Zeitdauer pro Tag beschränkt. Bei der Einstellung der Zeit nach Zeitabständen werden der Beginn und das Ende des Zeitraums angegeben, in dem der Zugang zum Internet möglich ist (nur an diesen bestimmten Tagen). So können Eltern genau festlegen, wann ihre Kinder im Internet surfen dürfen.

Schritt 8: Lernmodus starten



Durch Klicken auf die Schaltfläche „Ja“ wird der Lernmodus von SPHINX gestartet. Damit können Sie Ihre Kontrollregeln interaktiv konfigurieren. Für jede Datenübertragung, die nicht ausdrücklich in Ihren Kontrollrichtlinien angegeben ist, können Sie in SPHINX über ein Warnungsüberwachungsprogramm interaktiv festlegen, ob eine entsprechende Kommunikationskontrollregel aktiviert werden soll. So werden die Filterregeln Stück für Stück festgelegt. Durch Klicken auf „Nein“ wird der Lernmodus deaktiviert. Sie können aber jederzeit zu einem späteren Zeitpunkt in diesen Modus wechseln.

Schritt 9: Bestätigung der Sicherheitsrichtlinien



In diesem Menü können Sie sich einen Überblick über Ihre aktuellen SPHINX-Sicherheitsrichtlinien verschaffen und diese entweder bestätigen oder neu konfigurieren.
Um die zahlreichen Funktionen von SPHINX voll auszunutzen, sollten Sie später im Menü „Erweiterte Konfiguration" Ihre Konfigurationseinstellungen angeben.

4

Die SPHINX-Geheimnisse erkunden

4 Die SPHINX-Geheimnisse erkunden

4.1 Hauptkonsole

Nach der Installation der grafischen Benutzeroberfläche und der Filter-Engine von SPHINX kann die Konfiguration beginnen. Nach dem Klicken auf das SPHINX-Symbol wird das Startmenü angezeigt:



Über das Optionsfeld in dieser Konsole kann der Ausführungsmodus der SPHINX-Firewall schnell die folgenden Optionen aktivieren:

- **Zugang für alle zulassen:** In diesem Modus wird die gesamte Netzwerkkommunikation durchgelassen. Es erfolgt keine Kontrolle.
  In diesem Durchgangsmodus ist die Kontrolle durch SPHINX deaktiviert (dieser Modus kann für Wartungszwecke oder für die Netzwerkprüfung durch ein Prüf-Tool verwendet werden). Bitte beachten Sie, dass SPHINX in diesem Modus „Zugang für alle zulassen“ KEINERLEI Schutz bietet.
- **Zugang allen verwehren:** In diesem Modus ist die gesamte Netzwerkkommunikation unterbrochen, ohne dass feinere Unterscheidungen gemacht werden. Es handelt sich um einen kompletten Unterbrechungsmodus, in dem SPHINX jegliche Kommunikation unterbindet. Dieser Modus wird hauptsächlich für Wartung und Fehlersuche verwendet. „Zugang allen verwehren“ trennt den Computer vollständig vom Netzwerk, es findet keine Kommunikation mehr mit der Außenwelt statt. Mit diesem Modus können Sie den Zugang zu Ihrem Computer vom Netzwerk aus vollständig unterbinden.
- **SPHINX:** Im normalen SPHINX-Modus werden alle ankommenden/abgehenden Netzwerkdatenübertragungen kontrolliert, wobei die in der aktiven Konfiguration von SPHINX angegebenen Regeln Anwendung finden. Das ist der normale Betriebsmodus von SPHINX. Er ermöglicht die Kontrolle der Kommunikation zum und vom PC des Benutzers.
- Die zwei Fortschrittsbalken zeigen an, wie viele ankommende und abgehende Datenpakete nicht durchgelassen werden (Anzahl aller Datenpakete / Anzahl der nicht durchgelassenen Datenpakete). Ein roter Anzeigebalken bedeutet, dass sehr viele Datenpakete nicht durchgelassen werden. Ein roter oberer Anzeigebalken zeigt einen Angriff auf Ihren Computer bzw. Websites mit viel Werbung an. Ein roter unterer Anzeigebalken zeigt an, dass häufig versucht wird, auf Ihrem Computer auf Dienste zuzugreifen, auf die der Zugriff nicht erlaubt wurde, oder dass Ihr Browser versucht, auf Cookies zu antworten.

SPHINX bietet je nach Ihren Anforderungen und Ihren Firewall-Fachkenntnissen zwei Konfigurationsmodi:

- **Basiskonfiguration:** Dieser Modus ist für Benutzer geeignet, die keine verfeinerte Zugangskontrolle benötigen. Es werden die grundlegenden Konfigurationsfunktionen von SPHINX aktiviert.

- **Erweiterte Konfiguration:** Dieser Modus ist für Benutzer geeignet, die komplexe Kontrollregeln definieren möchten. Hier werden alle Konfigurationsfunktionen von SPHINX zur Verfügung gestellt. Es wird empfohlen, zuerst die Basiskonfiguration zu wählen und anschließend, wenn Sie sich mit den verschiedenen Firewall-Funktionen vertraut gemacht haben, zum erweiterten Modus überzugehen.
  Nach dem Klicken auf eine der Schaltflächen werden Sie von einem Einblendmenü durch die verschiedenen Konfigurationsfunktionen von SPHINX geführt.

4.2 Pull-Down-Menüs



4.2.1 Datei

Neben dem Laden und Speichern von Konfigurationen ist auch das Exportieren und Importieren von Teilen der gegenwärtig aktiven Konfiguration von anderen PCs möglich. Das ist besonders nützlich, wenn Sie einheitliche Kontrollrichtlinien auf mehreren PCs installieren möchten.

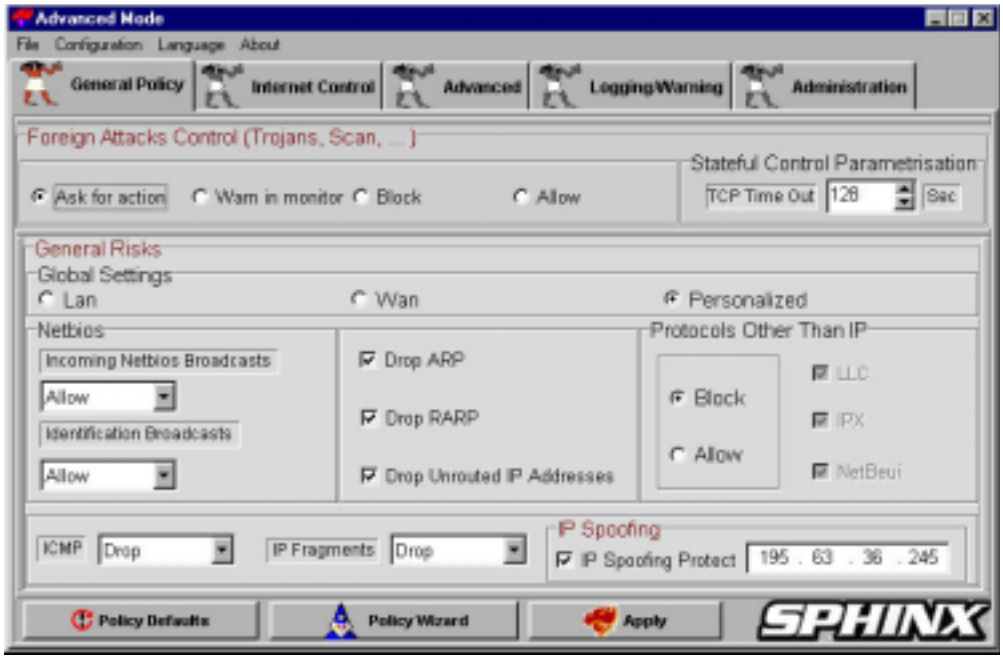


Wählen Sie den Teil der Konfiguration aus, den Sie wieder verwenden möchten, und klicken Sie auf die Schaltfläche „Export“, um ihn als Konfigurationsdatei zu speichern. Auf dieselbe Weise können Konfigurationen von anderen PCs durch Klicken auf die Schaltfläche „Import“ importiert werden.

4.2.2 Konfiguration

Nach jeder Änderung in der aktuellen Konfiguration können Sie diese übernehmen, indem Sie im <Konfigurationsmenü> auf die Schaltfläche <Übernehmen> klicken. Die aktuelle Konfiguration wird dann unmittelbar an den SPHINX-Treiber weitergegeben. Aus Sicherheitsgründen werden Änderungen nicht automatisch übernommen. Klicken Sie auf die Schaltfläche „Übernehmen“, wenn Sie die Firewall-Konfiguration abgeschlossen haben.

4.3 Konsole Allgemeine Richtlinien



Externe Angriffe (Scans, Trojaner)

SPHINX verwendet eine spezielle Statusüberwachungstechnologie, um feststellen zu können, ob Ihr PC von einem externen Rechner aus dem Internet oder Ihrem LAN angegriffen oder analysiert wird. Mit dieser Technologie können alle Arten von Hackerangriffen abgewehrt werden, nicht nur Angriffe auf TCP-Basis. Außerdem werden die gesamte externe IP-, UDP- und ARP-Kommunikation sowie Angriffe auf der Basis von Nicht-IP-Protokollen abgewehrt (IPX, NetBEUI).

- **Zulassen:** Wenn diese Option aktiviert ist, verhält sich SPHINX neutral und unterbindet keinerlei Kommunikation. Verwenden Sie diese Option mit Vorsicht, da in diesem Modus externe Angriffe und Scans nicht abgewehrt werden.
- **Sperren**: Diese Option aktiviert die Statusüberwachungstechnologie von SPHINX, gibt aber keine Warnmeldungen aus.
- **Sperren und Warnen:** Mit dieser Option können Sie externe Verbindungen blockieren und bei Hackerangriffen im Warnungsüberwachungsprogramm Warnmeldungen ausgeben lassen. Wenn SPHINX externe Verbindungsversuche feststellt, wird eine Warnung in der Konsole <Externe Verbindungsversuche> im Warnungsüberwachungsprogramm ausgegeben (siehe Warnungsüberwachungsprogramm). Zur genaueren Analyse können Sie dann Angriffe abwehren und diese im Warnungsüberwachungsprogramm genau untersuchen.
- **Sperren und Benutzerrückfrage:** Mit dieser Option können Sie externe Verbindungen sperren und über ein interaktives Einblendmenü für solche Angriffe auch interaktive Warnmeldungen ausgeben lassen. In diesem Einblendmenü werden auch die Angriffstools angegeben, die wahrscheinlich verwendet werden. Um die Flexibilität zu erhöhen, kann der Benutzer interaktiv entscheiden, welche Maßnahmen zu ergreifen sind (Sperren/Zulassen). Dies wird angeboten, falls ein erfahrener Benutzer eine eingehende Prüfung vornehmen will und einen Angriff mit bestimmten Netzwerk-Prüf-Tools (passive Angriffe) in Ihrer LAN-Umgebung genauer untersuchen möchte.

- **Zeitüberschreitung:** Ein grundlegender Parameter der Statusüberwachungstechnologie von SPHINX: ist eine Leerlaufzeit, nach der eine von Ihnen hergestellte Verbindung zu einem Remote-Server abgebrochen wird und alle Datenpakete von diesem Server als externe Verbindungsversuche interpretiert werden. Über diesen Wert kann der Benutzer die Statusüberwachungstechnologie für spezielle Fälle von langsamen WAN-Verbindungen kalibrieren. Bei einer sehr langsamen Netzwerkverbindung (bei der einige legitime Verbindungen durch Zeitüberschreitung abgebrochen werden) sollte dieser Wert erhöht werden.

Lernmodus

Mit diesen Funktionen können Sie Ihre eigenen Kontrollregeln erstellen. Für jede Datenübertragung, die nicht ausdrücklich in Ihren Kontrollrichtlinien angegeben ist, ermöglicht Ihnen SPHINX, interaktiv oder im Nachhinein (<Warnungsüberwachungsprogramm>) über den Einbau von Kontrollmechanismen in diese Kommunikation zu entscheiden. So können Sie Ihre Filterdatenbank im Lernmodus kontinuierlich aufbauen. Bei der Aktivierung des Lernmodus haben Sie die Wahl zwischen zwei exklusiven Richtlinien.

- Pessimistischer Modus: Im pessimistischen Modus (Blockmodus) BLOCKIERT SPHINX jede Kommunikation, die nicht von Ihren Sicherheitsrichtlinien abgedeckt ist, und ermöglicht Ihnen, eine entsprechende Kontrollregel hinzuzufügen.
- Explorativer Modus: Im explorativen Modus ERLAUBT SPHINX die Kommunikation, für die keine speziellen Regeln angegeben wurden. Dieser Modus ist für viele Internet-Dienste sinnvoll, z.B. für das Surfen im Internet. Sie können sich frei im Internet bewegen und nach der Analyse der Inhalte entscheiden, ob Sie den Zugriff auf Internet-Sites erlauben oder verwehren wollen. Diese Option ist besonders in Kombination mit weißen Listen sinnvoll. Damit können alle möglichen Verbindungen (Links usw.) von einer Site überprüft und auf einfache Weise entschieden werden, welche Verbindungen zugelassen werden sollen. Im <Interaktiven Modus> (Konsole Protokollierung / Konsole Warnungsüberwachungsprogramm) werden Einblendmenüs aller Datenübertragungen angezeigt, für die keine ausdrücklichen Filterregeln angegeben wurden (Internet-Kontrolle).

Wenn Sie sich im <Überwachungsprogrammmodus> befinden (Konsole Protokollierung / Warnungen), werden vom Protokollierungsüberwachungsprogramm alle Datenübertragungen angezeigt, für die keine ausdrücklichen Filterregeln angegeben wurden. Wenn sie auf diese Warnmeldungen klicken, werden Sie nach Ihrer Entscheidung gefragt (mit den gleichen Einblendmenüs). Wenn Sie verhindern wollen, dass ständig Einblendmenüs geöffnet werden, sollten Sie den letzten Modus wählen.

Allgemeiner Schutz vor Angriffen

Mit diesen Optionen können Sie die im Normalfall zu verwendende Kontrolle von Typen und Formen der Kommunikation angeben.

Kontrollkästchen ARP

Wenn Sie an ein LAN angeschlossen sind, ist es SEHR empfehlenswert, den ARP-Datenaustausch zuzulassen, da Ihr Computer sonst keinen Zugriff auf das LAN hat.

Kontrollkästchen ICMP

Wenn Sie über ein Modem mit dem Internet verbunden sind, sollten Sie ICMP-Pakete blockieren, die durch Informationen und Aktionen dieses Protokolls wie „Smurf-Angriffe“ oder DoS (Denial of Service)-Angriffe die Sicherheit Ihres Computers und auch anderer PCs gefährden können. Wenn Ihr Rechner an ein LAN angeschlossen ist, sollten Sie Ihren Sicherheitsadministrator fragen, welche Einstellung Sie vornehmen sollen, da der Einsatz dieses Protokolls auf dieser Netzwerkebene sinnvoll sein kann.

Kontrollkästchen FRAGMENTE SPERREN

Es wird empfohlen, diese Option zu aktivieren und fragmentierte IP-Pakete nicht durchzulassen. Manche Angriffe basieren auf Sicherheitslücken beim Wiederzusammensetzen von (IP) Kommunikationsmeldungen.

Kontrollkästchen NICHTGEROUTETE IP-ADRESSEN SPERREN
Es wird empfohlen, diese Option zu aktivieren und nichtgeroutete IP-Adressen nicht durchzulassen. Manche Angriffe basieren auf diesen Adressen. Falls Sie die nicht gerouteten IP-Adressen nicht in Ihrem lokalen Netzwerkbereich verwenden, z.B. einem LAN, sollten Sie Ihren Sicherheitsadministrator fragen, welche Entscheidung Sie treffen sollen.

Kontrollkästchen Schutz vor IP-SPOOFING
Es wird empfohlen, diese Option zu aktivieren, damit Ihr Computer nicht zum Ausgangspunkt von Angriffen auf andere Rechner werden kann. Mit Tools, die die Quell (IP)-Adresse Ihrer üblichen Kommunikation ändern (IP-Spoofing), ist es möglich, in andere Computer einzudringen (weitere Einzelheiten über diese Angriffsarten finden Sie in der Hilfedatei dieses Assistenten). Sie sollten sich bewusst sein, dass durch diese Option etwas mehr Overhead verursacht wird.

Feste Vergabe der lokalen IP-Adresse an ...
Diese Option ist in LAN-Umgebungen sinnvoll, da die Benutzer dadurch dadurch gehindert werden, die Ihnen zugeteilte IP-Adresse zu ändern. Benutzer, die eine IP-Adresse ohne Genehmigung durch den Administrator ändern, können nicht über das LAN kommunizieren. Die Verwendung der IP-Adresse eines anderen Rechners kann in manchen LAN-Umgebungen zu Problemen führen und kann außerdem bewusst für IP-Spoofing-Angriffe missbraucht werden.

Nicht-IP-Protokolle (IPX/SPX, NetBEUI)
Wenn Sie nur mit dem Internet verbunden sind und Ihr Rechner nicht Bestandteil eines Novell-LANs ist und sie keine Anwendung ausführen oder verwenden, die auf NetBEUI basiert (ein IBM-spezifisches Protokoll, das in einigen Microsoft-Umgebungen verwendet wird), wird empfohlen, die Kommunikation über andere Protokolle als IP zu deaktivieren.
Wenn Ihr Rechner an ein LAN angeschlossen ist, fragen Sie bitte Ihren Sicherheitsadministrator, welche Entscheidung die richtige ist.

4.4 Internet-Kontrolle



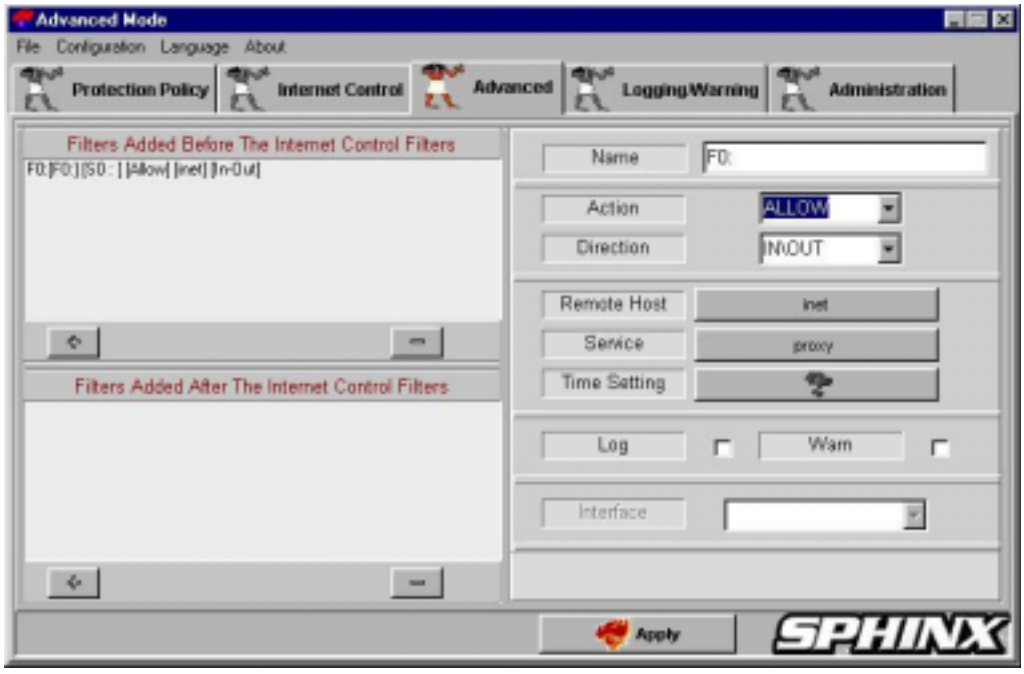
In dieser Konsole können vom Benutzer Kontrollregeln für eine Vielzahl von Internet-Diensten wie Web, FTP, Versenden von E-Mail, Empfangen von E-Mail, Chat, IRC usw. hinzugefügt werden. Standardmäßig sind alle Dienste zugelassen. Wählen Sie die Unterkonsole des Internet-Dienstes, für den Sie Kontrollregeln angeben möchten, und wählen Sie die gewünschte Kontrolle und Protokollierung:

Aktion

- **Beim Benutzer anfragen:** Wenn dese Option aktiviert ist, werden Sie gefragt (interaktiv oder im Überwachungsprogramm), ob Sie auf eine Website mit einem ausgewählten Internet-Dienst wie FTP oder IRC zugreifen wollen.
- **Alle zulassen:** Wenn diese Option aktiviert ist, kann auf ALLE Websites zugegriffen werden.
- **Alle sperren:** Wenn diese Option aktiviert ist, ist der Zugriff auf alle Websites gesperrt.
- **Schwarze Liste/weiße Liste:** SPHINX ermöglicht Ihnen die Wahl zwischen zwei Zugriffskontrollstrategien:
- **Schwarze Liste:** In diesem Modus ist der Zugriff auf alle ANDEREN Websites möglich, die nicht im Fenster für die schwarze Liste angegeben sind.
  Die in der schwarzen Liste eingetragenen Websites werden gesperrt.
- **Weiße Liste:** In diesem Modus ist der EXKLUSIVE Zugriff auf Websites möglich, die im Fenster der weißen Liste angegeben sind. Alle anderen Websites werden gesperrt.

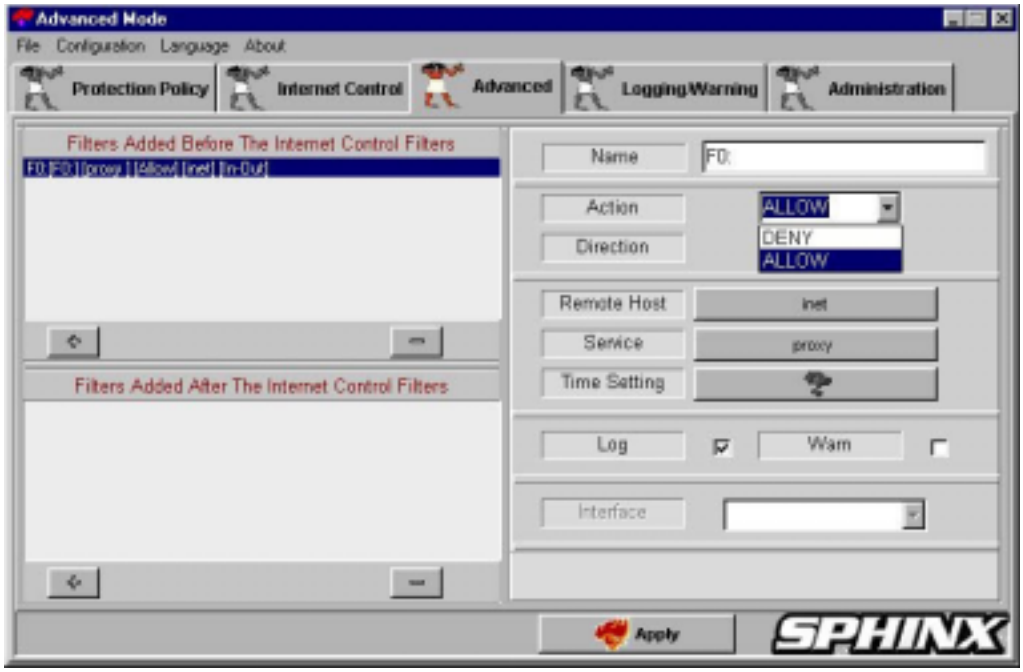
Die Internet-Kontrollfunktionen bieten einen effektiven Mechanismus für die Zugriffskontrolle durch Eltern und Bildungseinrichtungen. Klicken Sie zum Einrichten und Aktualisieren Ihrer schwarzen und weißen Listen einfach auf die Schaltflächen „Hinzufügen“, „Löschen“ und „Ändern“. Websites können durch ihre URL (Internet-Sites) oder IP-Adressen angegeben werden (LAN). Weiterhin können komplette URL-Listen importiert bzw. exportiert werden. Mit der Konsole Internet-Kontrolle können Sie schwarze Listen einrichten, in denen die URLs von Websites mit radikalen, pornografischen oder gefährlichen Inhalten abgelegt sind. Als Alternative können auch alle URLs gesperrt werden und nur spezielle, in der weißen Liste aufgeführte Websites zugelassen werden.

4.5 Erweiterte Konfiguration



Dieses Menü kann von Benutzern verwendet werden, die über gute Kenntnisse von Protokollen und Filterregeln verfügen. SPHINX bietet hier die Leistungsfähigkeit einer professionellen Firewall und ermöglicht erweiterte Konfigurationsmöglichkeiten zur Kontrolle der gesamten Kommunikation. Sie können Ihre eigenen Netzwerkdienste definieren und Filter erstellen, die von der Konsole Internet-Kontrolle aus angewendet werden können. Die ausgewählten Filter können auf spezielle Tage und Uhrzeiten oder für spezielle Zeiträume während des Kommunikationsaustauschs eingestellt werden. Dadurch können Sie festlegen, wie lange die Benutzer Zugriff auf Dienste haben.

Um spezielle Dienste zuzulassen, müssen die folgenden Schritte durchgeführt werden: Die Filtertabelle von SPHINX arbeitet nach dem „Prinzip des ersten Treffers“. Wenn ein Netzwerkpaket vom PC empfangen wird, prüft SPHINX die Filtertabelle von oben nach unten, d.h., die Reihenfolge der Filterzeilen ist sehr wichtig. Wenn z.B. im Fenster „Filter, die vor den Internet-Kontrollfiltern hinzugefügt wurden" HTTP in beiden Richtungen gesperrt ist, kann HTTP nicht funktionieren, da es vor den Internet-Kontrollfiltern gesperrt wird. Klicken Sie zum Starten des Vorgangs auf die Schaltfläche „+“. Das folgende Fenster wird geöffnet:



Name : Jede Filterzeile hat ihren eigenen Namen.

Aktion : Durch Klicken auf den Pull-Down-Pfeil wird das Pull-Down-Aktionsmenü geöffnet. Der Anwender kann wählen, ob Dienste oder Protokolle zugelassen oder gesperrt werden sollen.

Remote-Rechner : Durch Klicken auf das Fragezeichen unter „Remote-Rechner“ wird die folgende Konsole geöffnet:



Hier können die Benutzer den Remote-Rechner angeben, für den dieser Dienst zugelassen oder gesperrt werden soll. Es kann entweder die URL oder die IP-Adresse des Remote-Rechners angegeben werden. Bei Angabe der URL muss der Domain-Name-Service bereits zugelassen sein. Bei Angabe der IP-Adresse sind noch einige andere Angaben möglich. Wenn das Kontrollkästchen „Alle Adressen“ aktiviert ist, wird der angegebene Dienst für alle Adressen, also das gesamte Internet zugelassen oder gesperrt.

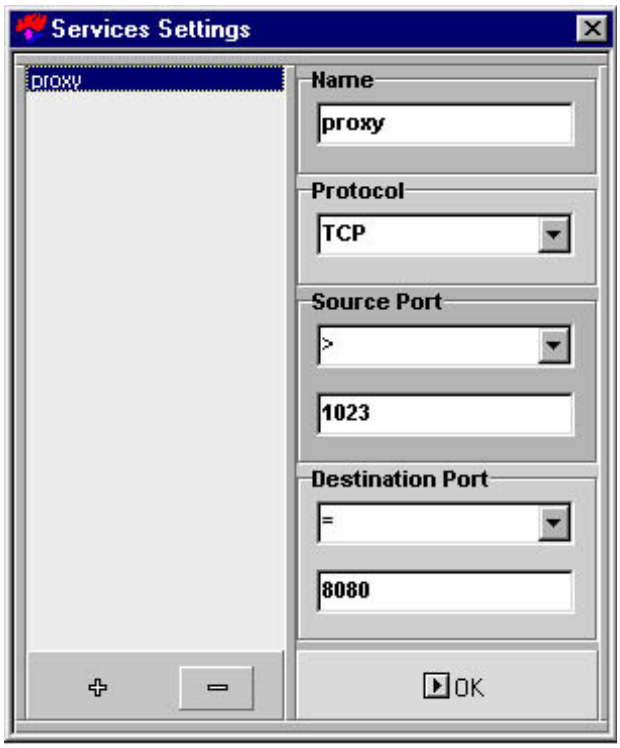


Es ist möglich, konkrete IP-Adressen, ein ganzes Netzwerk oder ein Teilnetzwerk (durch die Netzwerkmaske definiert) zu verwenden. Im Fall eines einzelnen Rechners muss die Netzwerkmaske auf 255.255.255.255 eingestellt werden.



In diesem Fall ist nur eine IP-Adresse ausgewählt. Der Dienst in dieser Filterzeile wird nur für die IP-Adresse 151.189.0.158 zugelassen oder gesperrt.

Durch Klicken auf die Schaltfläche „Dienst“ wird das folgende Fenster geöffnet



Im Feld „Name“ wird der Name des Dienstes festgelegt. Durch Klicken auf den Pull-Down-Pfeil wird das Protokoll-Pull-Down-Menü geöffnet. Die folgenden Protokolle können ausgewählt werden: IP, TCP, UDP, FRAGMENT und ICMP.

Protokollierung von Aktivitäten

Für jeden Dienst gibt es verschiedene Protokollierungsoptionen:

- ALLE: Alle Aktivitäten werden protokolliert.
- Gesperrt: Nur Zugriffsversuche auf gesperrte Websites werden protokolliert.
- Zugelassen: Nur Zugriffsversuche auf zugelassene Websites werden protokolliert.

4.6 Konsole Protokollierung / Warnung

In dieser Konsole können verschiedene Protokollierungs- und Warnrichtlinien definiert werden. Die Benutzer können die Protokollierung und Warnung standardmäßig begrenzen, auch wenn diese in den verschiedenen SPHINX-Menüs aktiviert wurden.



Allgemeine Warnungen

Mit diesen Einstellungen kann angegeben werden, ob die Warnungsmeldungen aktiviert oder deaktiviert werden sollen. Die Benutzer können entscheiden, ob interaktive Einblendmenüs verwendet werden oder ob die Warnmeldungen an das Warnungsüberwachungsprogramm weitergeleitet werden sollen.

1. ALLE Warnungen aktivieren: Wenn Sie dieses Kontrollkästchen deaktivieren, gibt SPHINX keine Warnmeldungen an Sie aus.
2. Überwachungsmodus / Interaktiver Modus: Wenn der interaktive Modus aktiviert ist, werden Warnmeldungen, nicht definierte Datenströme und externe Verbindungsversuche durch Einblendmenüs angezeigt. Diese Option wird automatisch auf den Überwachungsmodus eingestellt, wenn der versteckte Modus von SPHINX aktiviert ist (Konsole <Administrator>, siehe unten), bei dem SPHINX im Hintergrund ausgeführt wird.

Allgemeine Protokollierung

Mit diesen Einstellungen können die ALLGEMEINEN Protokollierungsrichtlinien angegeben werden:

1. Protokollierung Internet-Kontrollfilter aktivieren: Wenn dieses Kontrollkästchen aktiviert ist, werden alle Aktivitäten von Internet-Diensten wie FTP oder IRC protokolliert. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird keine Protokollierung durchgeführt.

2. Protokollierung erweiterte Filter aktivieren: Wenn dieses Kontrollkästchen aktiviert ist, werden alle Filter protokolliert, für die Sie die Protokollierung angefordert haben. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird keine Protokollierung durchgeführt.
3. Tägliche Sicherung als separate Datei: Mit dieser Option können Sie angeben, ob die protokollierten Daten an jedem Tag der Woche in einer neuen Datei gespeichert oder in einer gemeinsamen Datei an einem anderen Speicherort gespeichert werden sollen.

Einstellungen Protokolldatei

Um den Benutzern umfangreiche Einstellungsmöglichkeiten für den Protokollierungsvorgang zu geben, werden in dieser Unterkonsole verschiedene Funktion zum Schutz gegen Angriffe angeboten. Maximale Größe der Protokolldatei: Angabe der maximalen Größe der Protokolldatei. **Wenn Protokolldatei voll:** Angabe, welche Aktion durchzuführen ist, wenn die Protokolldatei voll ist.

Datei überschreiben: Die vorherigen Protokolle werden gelöscht, und eine neue Protokolldatei wird angelegt. Dieses Ereignis wird im Protokollierungsüberwachungsprogramm unter der Konsole <Systemwarnungen> angezeigt.

Alle sperren: SPHINX sperrt die gesamte Kommunikation und erstellt kein Protokoll mehr.

Keine Protokollierung mehr: Standardmäßig kontrolliert SPHINX den Datenverkehr, erstellt aber kein Protokoll.

Protokoll auf Festplatte speichern: Besonders auf langsamen PCs kann das Speichern von Daten auf der Festplatte die anderen Aktivitäten verzögern. In SPHINX können die Zeitintervalle angegeben werden, nach denen die Protokolldateien auf der Festplatte gespeichert werden. Dazwischen werden die Protokolldateien lediglich im Hauptspeicher gespeichert.

4.7 Konsole Administration



Zeitangabe Internet-Verbindungen

Mit dieser Option kann angegeben werden, zu welcher Uhrzeit PC-Benutzer das Netzwerk für Internet-Dienste nutzen können.

Passworteinstelllungen

Durch Klicken auf „Passwort ändern“ öffnet sich das folgende Einblendfenster:



Das SPHINX-Passwort kann durch Eingabe des alten und neuen Passworts geändert werden.

Betriebsmoduseinstellungen

versteckter Modus von SPHINX:
SPHINX kann im versteckten Modus ausgeführt werden. Auf diese Weise kann die Kontroll- und Aktivitätsprotokollierung durchgeführt werden, ohne dass die Benutzer das Programm bemerken. Die Aktivierung dieser Option ist nützlich, um ohne Wissen der Benutzer die Aktivitäten an einem PC zu überprüfen, der an das Netzwerk angeschlossen ist. Um diesen Modus zu aktivieren und zu verhindern, dass die Benutzer das SPHINX-Standardsymbol erkennen und dadurch wissen, dass das Programm auf dem PC installiert ist, wird empfohlen, das Sphinx-Standardsymbol zu ändern und ein anderes Symbol aus der Liste der verfügbaren Symbole auf Ihrem PC auszuwählen. Dasselbe gilt für das Fenster von Sphinx.

WICHTIG: Um in das Anmeldefenster von SPHINX zu gelangen, müssen STRG und Leertaste gleichzeitig gedrückt werden. Anschließend kann das SPHINX-Passwort eingegeben werden, um in den Konfigurationsmodus von SPHINX zu gelangen.

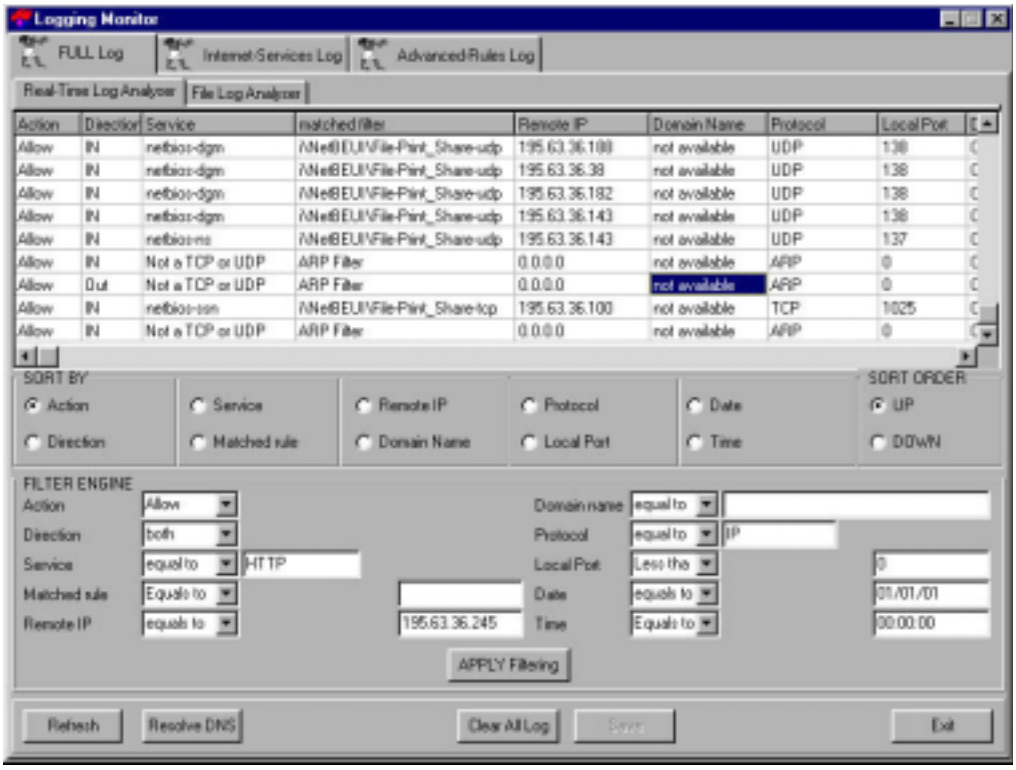
Konfigurationsdatei verschlüsseln:
Es wird empfohlen, Ihre Konfigurationsdateien zu verschlüsseln (falls Ihre lokalen Verschlüsselungsrichtlinien das zulassen), um zu verhindern, dass jemand Ihre Konfigurationsdateien sehen oder ändern kann, und um zu verhindern, dass anstatt Ihrer eigenen Konfigurationsdateien andere Konfigurationsdateien auf Ihrem lokalen PC aktiviert werden.

Immer letzte Konfiguration laden
Mit dieser Option kann die zuletzt geladene Konfiguration (vorangegangene Sitzung) automatisch geladen und aktiviert werden.

4.8 Protokollierungsüberwachungsprogramm

Das Protokollierungsüberwachungsprogramm verfügt über drei Unterkonsolen:

1. Protokoll Internet-Dienste: Erstellung von Protokollen nur entsprechend den Internet-Kontrollrichtlinien <Konsole Internet-Kontrolle>, sortiert nach Diensten.
2. Protokoll nach erweiterten Regeln: Erstellung von Protokollen entsprechend den Regeln der Konsole <Erweiterte Kontrolle>.
3. Konsole mit vollständiger Protokollierung: In dieser Konsole werden alle registrierten Protokollereignisse angezeigt. In den bisher erwähnten Konsolen können ausgewählte Teile der Protokolldateien untersucht werden (Internet-Kontrolle / Erweitert), in dieser Konsole jedoch wird die genaue Abfolge der Protokollereignisse angezeigt (Internet-Kontrolle / Erweitert).



Echtzeitprotokollanalyse
In dieser Konsole wird die Protokollierung der aktuellen Sitzung in Echtzeit angezeigt. Zur zusätzlichen Analyse können die Sortier- und Filterfunktionen verwendet werden (siehe unten).

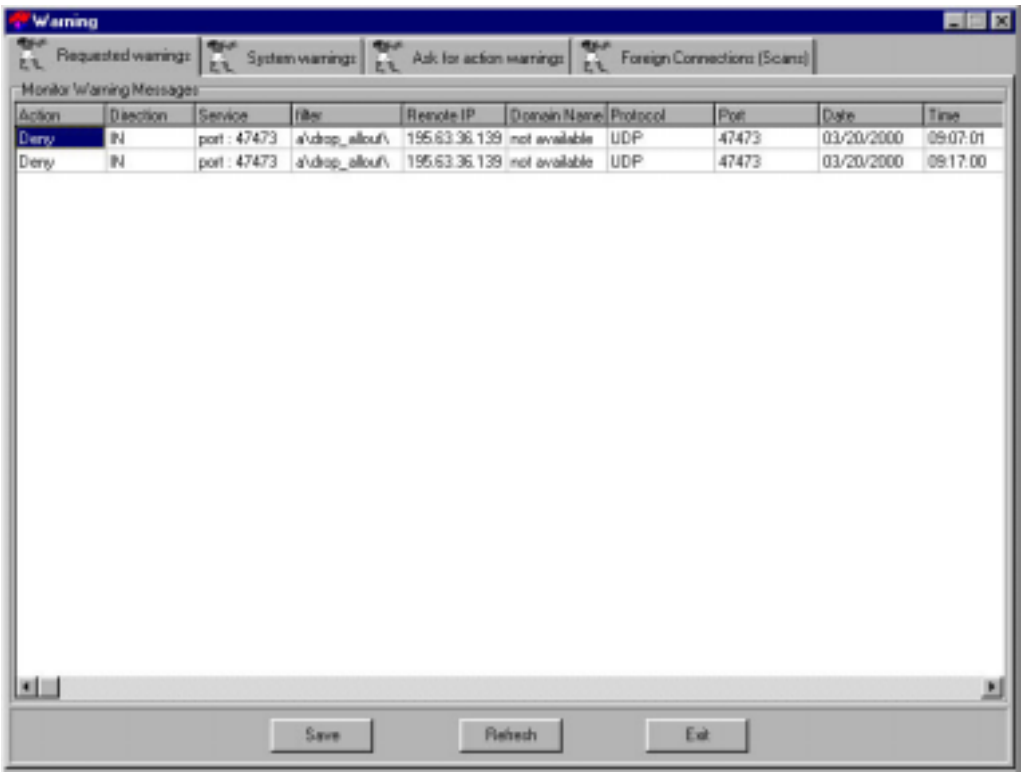
Protokolldateianalyse
Mit dieser Konsole können vorher gespeicherte Protokolldateien geladen und mit den Sortier- und Filterfunktionen analysiert werden.

Allgemeine Dienstprogramme
DNS-Auflösung: Diese Option listet die mit den in den Protokollverknüpfungen registrierten IP-Adressen verknüpften URLs auf und ermöglicht damit die detaillierte Untersuchung von Protokolldateien. Bei dieser Option wird davon ausgegangen, dass ein DNS-Server verfügbar ist (oder dass Sie mit dem Internet verbunden sind) und kann viel Zeit in Anspruch nehmen, wenn die Protokolldateien groß sind bzw. Ihre Internet-Verbindung langsam ist.

Aktualisieren: Um die Verzögerung von Benutzeraktivitäten zu vermeiden, ruft SPHINX regelmäßig Protokollierungsdaten ab.
ALLE Protokolle: Klicken Sie auf diese Schaltfläche, um alle vorhandenen Protokolldateien zu löschen. Bitte beachten Sie, dass dadurch alle aktuell registrierten Protokolldateien gelöscht werden.
Drucken: Drucken der aktuellen Protokolldateien.

Funktionen zum FILTERN und SORTIEREN
SORTIEREN NACH: Mit dieser Funktion können die Protokolldateien in aufsteigender oder absteigender Reihenfolge sortiert werden (Optionsfeld REIHENFOLGE FESTLEGEN). Die Sortierfolge bezieht sich auf alle Felder der Protokollierungszeile (Aktion / Remote-IP).
FILTER-ENGINE: SPHINX bietet vielfältige Filterfunktionen, mit denen Protokollzeilen ausgefiltert werden können. Sie können FORTSCHREITENDE Filter anwenden (der nächste Filter wird auf das Ergebnis des vorherigen Filters angewendet usw., um die selektive Kontrolle des Protokollvorgangs zu ermöglichen). Klicken Sie zum Aktivieren eines konfigurierten Filters auf die Schaltfläche „Filter anwenden“.

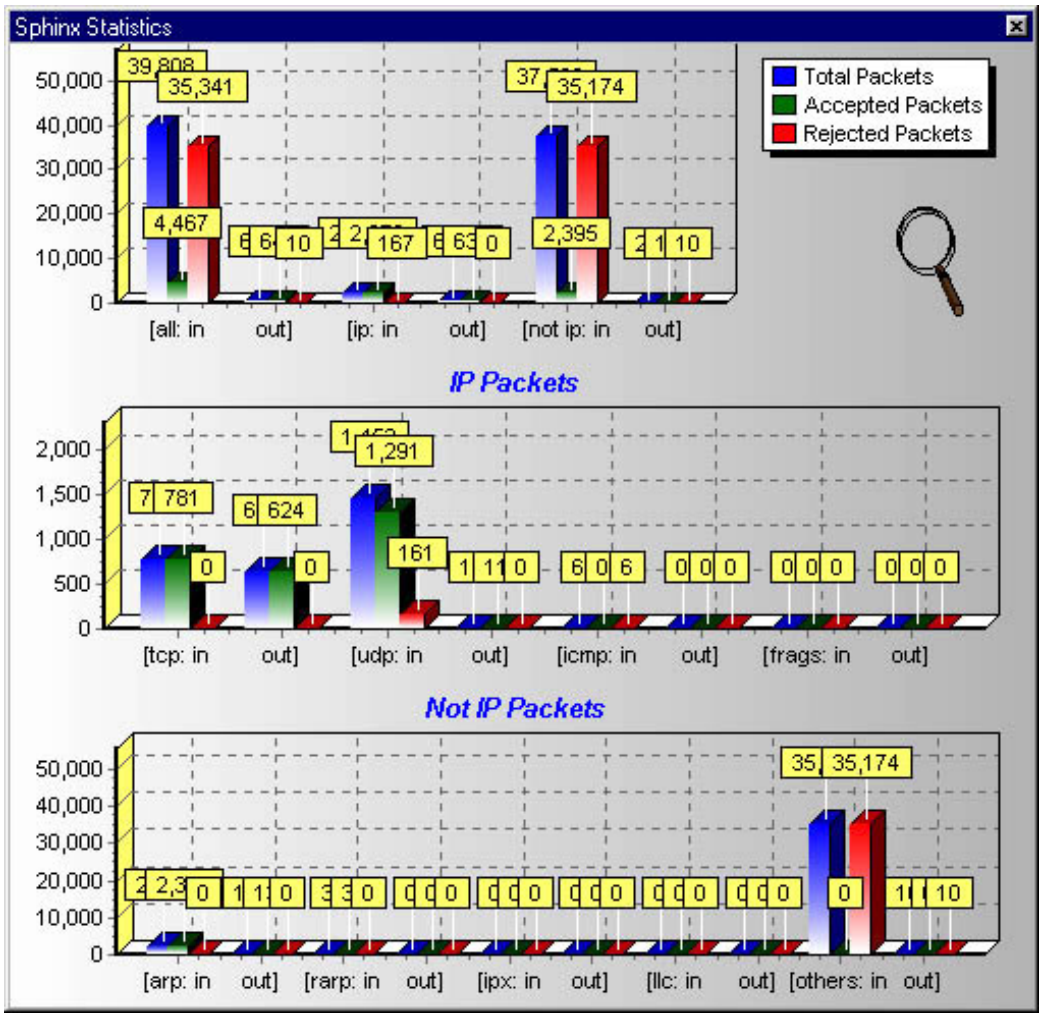
4.9 Warnungsüberwachungsprogramm



Das Konzept des Warnungsüberwachungsprogramms ermöglicht dem SPHINX-Administrator, Warnmeldungen zu registrieren. Wenn Sie durch Auswahl des Überwachungsmodus in der Konsole <Protokollierung / Warnung> festlegen, dass Warnmeldungen (Lernmodus und externe Verbindungsversuche) zum Protokollüberwachungsprogramm geleitet werden sollen, werden diese Meldungen im Warnungsüberwachungsprogramm registriert. Sie können sie dann später offline oder innerhalb einer Prüfoperation anzeigen.

1. Lernmoduswarnungen: Wenn der Lernmodus aktiviert ist, können Sie hier Filterzeilen für verschiedene Netzwerkdatenpakete erstellen. Alle Datenübertragungen mit nicht definierten Kontrollregeln werden aufgeführt.
2. Warnungen bei externen Verbindungen: Durch Auswahl einer der Schaltflächen „Sperren und warnen“ bzw. „Sperren und Benutzer fragen“ können Filterzeilen für den Rechner erstellt werden, von dem die Datenpakete stammen.
3. Ausgegebene Warnungen: Beim Protokollieren der Diensteaktivitäten im erweiterten Kontrollmodus werden in diesem Menü die einzelnen Warnungen angezeigt.
4. Systemwarnungen: In diesem Menü werden Warnungen angezeigt, die sich auf die Ausführung von SPHINX selbst beziehen. Die Software gibt Meldungen aus, wenn nicht mehr in die Protokolldateien geschrieben werden kann, der freie Festplattenplatz zu gering wird oder wenn Benutzer versucht haben, sich bei SPHINX mit einem falschen Passwort anzumelden. Das Menü zeigt auch Benutzeraktionen, wie das Laden von Konfigurationen und das Festlegen von Regeln im Lernmodus an.

4.10 Statistikkonsole



Mit dieser Funktion können einige Statistiken zu den verschiedenen Netzwerkdatenübertragungen überprüft und über die von SPHINX nicht durchgelassenen Daten (Anzahl der nicht durchgelassenen Datenpakete / Anzahl der durchgelassenen Datenpaket in beiden Richtungen) berichtet werden. Damit ist eine unmittelbare Beobachtung der Anzahl der vom SPHINX-Kontrollmechanismus nicht durchgelassenen Daten möglich.