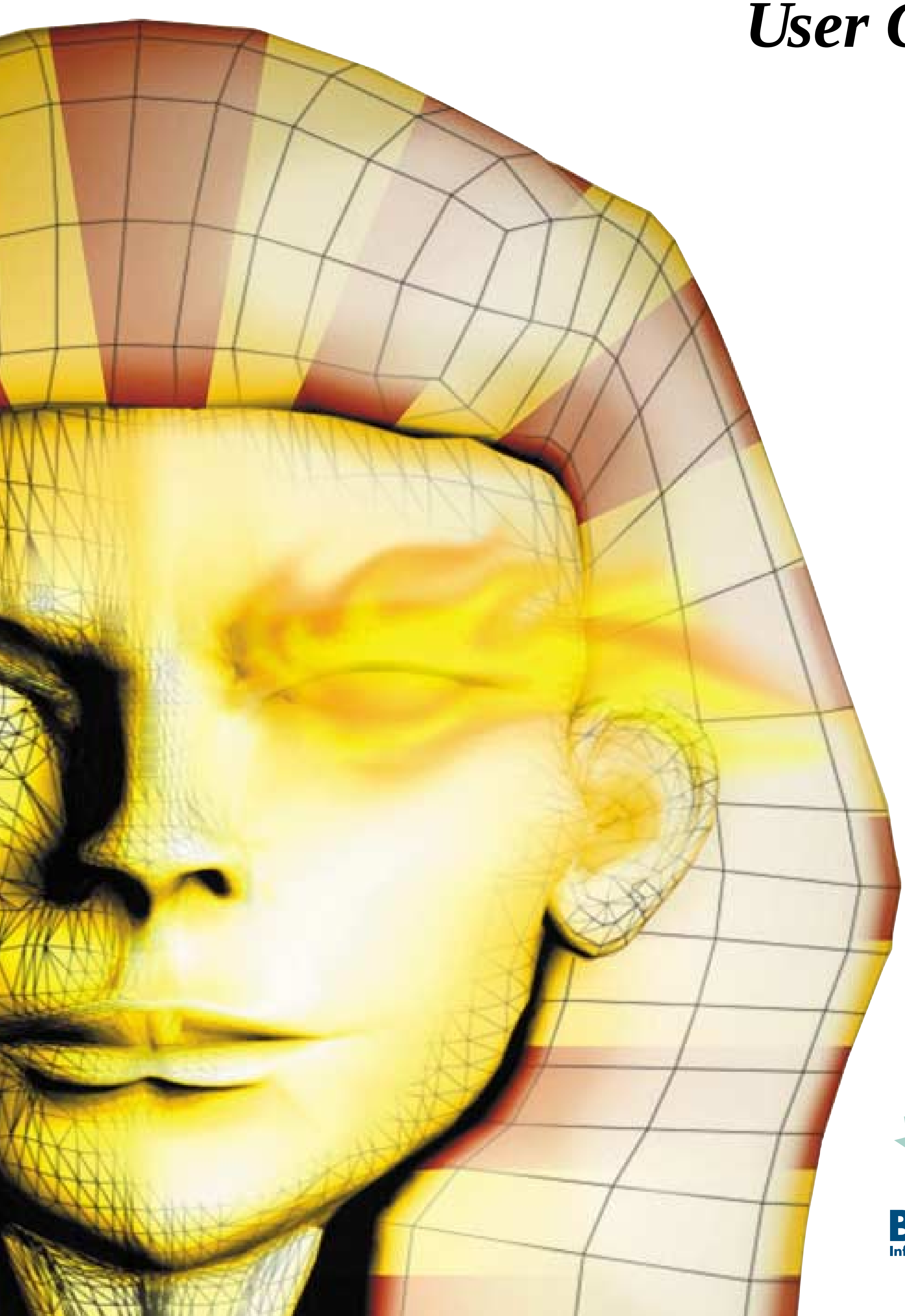
SPHINX PC Firewall

User Guide



Biodata
Information Technology

This software product (“SPHINX” program package) is subject to the provisions in the end-user license agreement that you can find either in the User’s Guide or in online format in the software itself.

By using the software, you acknowledge that you have read and accepted the terms and conditions of the license agreement.

Copyright Notice

Copyright © 2000 Biodata Information Technology AG.

All rights reserved.

This User Guide is protected by copyright law.

Online Registration

In order to receive the latest product information and details of updates, you must register this product with Biodata Information Technology AG.

You can now do this easily online at our Internet registration page. Please register yourself now (www.pcfirewall.com).

SPHINX End-User License Agreement for Program Packages

Please read the following License Agreement.
You must accept the License Agreement before using “SPHINX”.

END-USER LICENSE AGREEMENT FOR “SPHINX” PERSONAL FIREWALL

IMPORTANT – PLEASE READ CAREFULLY

CAUTION: This program is subject to the copyright laws of the Federal Republic of Germany and the provisions of international agreements. Any reproduction or unauthorized distribution of this program, wholly or parts thereof, is punishable by law. Any such unauthorized reproduction or distribution shall be prosecuted under civil and criminal law and is severely punishable and can lead to damage compensation claims.

The “SPHINX” software product is licensed and not sold.

This end-user license contract is a lawful agreement between yourself, the end-user (buyer), and Biodata Information Technology AG (lawful owner and producer).

The program package acquired by the buyer contains the above named “SPHINX” computer program on a machine-readable data carrier (CD-ROM) and the pertinent User’s Guide. The program and User’s Guide are protected by copyright law.

With the acquisition of this program package, the lawful owner grants the buyer the right to use the program under the terms and conditions for use stated herein. Any further use or exploitation is prohibited.

If the buyer acquires a computer on which the above named program is pre-installed, then the conditions and terms of using the program shall apply accordingly to the pre-installed duplicate of the program.

If the buyer does not agree to these conditions and terms of use, then the program package can be returned to the seller and the purchase price paid shall be refunded in full.

By using this software, you acknowledge that you accept these terms and conditions of the license agreement.

This end-user license agreement grants you the following rights (licensed rights):

General Terms and Conditions of Use

§1 Scope of Use

(1) The buyer is entitled to use the program on only one computer at any given time. The buyer is free to choose the computer on which the program shall be used. Use of the program is defined as being any lasting or temporary, wholly or partial, reproduction (duplication) of the program by storing, loading, running or display for the purpose of executing the program and processing of data contained in the program by the computer. The buyer is also entitled to undertake these operations for the purpose of observing, examining and testing the program. The User's Guide may not be reproduced in any form whatever.

(2) The program may be modified or adapted if this is necessary for the properly intended use, for linking the program with other programs or for correction of errors. Company names, trade marks, copyright notices and other notices concerning reservation of rights contained in the program may not be altered and must be incorporated unchanged into any modified or adapted versions of the program.

(3) Decompilation of the program code is only permitted under observance of the statutory restrictions pursuant to Article 69e Copyright Law of the Federal Republic of Germany (UrHG). Any other decompliation is prohibited.

(4) The buyer is entitled to produce a backup duplicate of the program if this is necessary to secure the future use of the program. If the program is copy-protected and the delivered program is damaged, then the customer can return the machine-readable data carrier supplied as part of the program package to the seller who will then supply a replacement copy.

§2 Transfer to Subsequent Users

(1) The buyer is entitled to transfer the program package in its original condition and entirety, together with a copy of this agreement, to a subsequent user. This entitlement does not extend to passing on copies or partial copies of the program and also not to passing on the modified or adapted versions or copies or partial copies thereof.

(2) The entitlement to use the program pursuant to Article 1 passes with the transfer of the program package to a subsequent user who then assumes the obligations of the buyer according to the meaning of this agreement. The buyer's entitlement to use the program pursuant to Article 1 extinguishes simultaneously.

(3) On transfer, the buyer must immediately and completely delete or otherwise destroy all copies and partial copies of the program, as well as modified or adapted versions and copies thereof. This shall also apply to all backup copies that may have been made.

(4) Paragraphs (1) to (3) shall also apply if the transfer is for temporary use. Renting out the program package or parts thereof is prohibited.

§3 Transfer by Subsequent Users

Transfer by the current user of this program package to any subsequent user implies that the subsequent user assumes the obligations of the preceding user. Article 2 shall apply accordingly.

§4 Other Rights

(1) All further rights of use and implementation of the program package are reserved. The buyer or subsequent users are especially not entitled to use the program and / or modified or adapted versions thereof on more than one computer at any given time or to distribute copied parts of the program package in its original state or in modified or adapted versions, even if such copied parts are restricted to essential parts of the modified versions. The exploitation rights of the buyer to own programs developed and operated in connection with the intended and proper use of the above stated program, as well as all other results obtained through use of the program, remain hereby unaffected.

(2) Following the release of a new version of the program, the buyer has the right to exchange the program package in return for a corresponding program package of the new version at the scheduled update price specified by the seller. The exchange is subject to the program package in its entirety as acquired by the buyer. The buyer's entitlement to use the original program pursuant to Article 1 extinguishes on the date of exchange. The obligation to delete and destroy pursuant to Article 2, paragraph 3 shall apply accordingly.

§5 Warranty

(1) Attention is drawn to the fact that it is not possible to develop computer programs in such a way that they work error-free under all application conditions. The seller warrants that the program is usable according to the program description issued at the point in time of delivery to the buyer and that it has the characteristics assured in the program description. An insignificant shortcoming in usability shall not be taken into consideration.

(2) The seller warrants that the original program is recorded on a tested data carrier, but no warranty is given for pre-installed programs.

(3) If the programme package proves unusable in the meaning of paragraph (1) or defect in the meaning of paragraph (2) then, within the six months' warranty period that begins on the date of delivery of the program package to the buyer, the program package may be returned to the seller who will deliver a new program package of the same name in exchange. In the event that this replacement also proves to be unusable in the meaning of paragraph (1) or defect in the meaning of paragraph (2) and if the lawful owner is unable to secure the usability with reasonable efforts within an appropriate period of time, then the buyer or user is entitled to choose between either a reduction of the buying price or return of the program package and refund of the purchase price. Article 2, paragraphs (2) and (3) shall apply accordingly.

(4) No further reaching warranty is given. Especially no warranty is given for the suitability of this program package for the particular requirements of the buyer or user. The buyer bears the sole responsibility for selection, installation and use, as well as for the therewith intended results. There is further no warranty whatever for modified or adapted versions of the programme pursuant to Article 1, paragraph (2), unless it can be proven that existing defects are in no way related to the modifications or adaptations.

§8 Liability

(1) Irrespective of the legal grounds, the seller and lawful owner are liable for damage caused by a breach of a significant contractual obligation for which they are responsible and that endangers fulfilment of the purpose of the agreement. The liability is restricted to the contractually typical damage, the occurrence of which the contractor must have taken into consideration on contract conclusion due to the circumstances known to him at that point in time. In no case shall the liability exceed five times the amount of the license remuneration. No liability is accepted for lost profits, unrealised cost savings or incidental and consequential damage.

(2) The liability restrictions stated in paragraph (1) do not apply to damage due to wilful conduct, gross negligence or the lack of assured characteristics or to any claims pursuant to Federal German Product Liability Law.

§9 Examination and Complaint Duty

(1) The buyer is obligated to examine the supplied program package for obvious defects easily noticeable by an average buyer. Complaints regarding obvious defects, especially missing data carriers or user's guides, as well as regarding significant and easily visible damage to the data carrier, are to be lodged in writing with the seller or lawful owner within two weeks following delivery. You will find the lawful owner's address in the User's Guide. The defects, especially the symptoms that have appeared, should be described as closely as possible.

(2) The buyer must lodge complaints regarding defects not immediately apparent with the seller or lawful owner within two weeks of their recognition.

(3) Neglect of the examination and complaint duty implies approval of the program package, despite the defect in question.

§10 Governing Law

(1) If you have acquired this product in Germany, then this end-user license agreement is subject to the laws of the Federal Republic of Germany.

(2) If you have acquired this product in Austria, then this end-user license agreement is subject to Austrian law.

(3) If you have acquired this product in Liechtenstein, then this end-user license agreement is subject to the laws of the Duchy of Liechtenstein.

(4) If you have acquired this product in Switzerland, then this end-user license agreement is subject to Swiss law.

(5) If you have acquired this product outside one of the above countries, then the locally applicable laws may possibly apply.

Table of Contents

1 Introduction: 6

2 Start SPHINXing 9

3 Making PCs Secure 11

4 Exploring the SPHINX Mysteries… 17

4.1 Main Panel 18

4.2 Pull-Down Menues 19

4.2.1 File 19

4.2.2 Configuration 19

4.3 General Policy Panel 20

4.4 Internet Control 22

4.5 Advanced Configuration 23

4.6 Logging / Warning Panel 26

4.7 Administration Panel 27

4.8 Logging Monitor 28

4.9 Warning Monitor 29

4.10 Statistics Panel 30

1

Introduction

1 Introduction:

SPHINX, the revolutionary Personal Firewall, is a software firewall solution designed to protect single desktop and notebook PCs both in Local Area Networks (LAN) and Wide Area Networks (WAN). With this protection tool, Biodata offers a flexible combination of security mechanisms in insecure environments. SPHINX protects home users' standalone PCs or computers in company networks against attacks.

For dial-up users or those on small networks without the benefit of a corporate firewall, SPHINX offers the most efficient and cheapest protection tool against attacks, Trojans and scans. It also enables users to have complete control of all network access to and from their PC: Moreover, a perimeter firewall by its own does not provide adequate protection and is not able to protect users' internal networks. It is open to any attack from within. SPHINX stops attacks inside the network and also applies an internal access policy between LAN stations.

SPHINX is an innovative PC firewall, which will enable you to efficiently protect your Desktop (Windows 98/ Windows NT/Windows 2000) from attacks and scans from unauthorized outside sources. SPHINX is also capable of controlling Internet access to school children, students or employees.

SPHINX offers the following characteristics:

Secure and Efficient

Biodata's SPHINX operates at the lowest level in the network stack, thus protecting the operating system and all applications above it from any packets delivered over the network interface. Since it runs in kernel mode, which it consolidates, it offers the best performance and protection against attacks, even attacks that target the operating system and its services. Unlike other desktop firewall products that are limited to securing only Winsock based applications, SPHINX provides network security for all PC communications. SPHINX filters all data packets by capturing them at the device (link layer) level, including IP (TCP, UDP, ICMP, NetBEUI, etc) protocols. So, it stops everything at the "entrance door" to the network.

Easy to Configure and Use

- *Wizard:* SPHINX includes a set of Wizards that allow for smart configuration, up to expert user level.
- *Automatic Learning Mode:* SPHINX includes the option of generate rules on the fly. In its automatic learning mode, SPHINX will explain the contents of each communication as well as the associated risks of allowing the packet through, so that novices can benefit from a simple and comprehensive rule learning mode to generate filtering rules easily. It also offers innovative ways of learning (Interactive or Monitor Mode / Explorative or Cautions Mode) which enables users to select the more convenient and cumbersome mode. Identification of the nature of the communication and resolution of IP addresses to URLs are also offered to help the user to understand the flows.
- The concept of *Warning Monitor* can make this learning mode less cumbersome for users by enabling the examination of accessed sites in a deferred manner and then the subsequent decision regarding their access (with the possibility of introducing a temporary testing phase.)
- *Explorative Mode* allows the user to examine the content of sites and to easily decide on the control to be applied to them.
- *Internet Services Control:* Original concept of White and Black Lists of URLs. SPHINX enables users to specify access control policies for each used Internet service (Web, Chat, News, Telnet, FTP etc.) allowing the specification of URLs to block (Black List) or access (White List Concept). Lists of prohibited sites can be imported easily from predefined lists of URLs.

Rich Logging and Warning Functions

- *Smart Logging:* SPHINX allows efficient, constant and rich logging for all traffic passing in or out of the PC with a set of auditing functions, offering possibilities of sorting and filtering of logs as well as the translation of IP addresses to relative URLs. Logged records are presented in a structured manner to facilitate their efficient and rapid examination.
- *Remote Logging:* SPHINX offers administrators the option to specify remote centralized logging. SPHINX logs at the entry door of the station removing the possibility of denying them by the end user (IP Spoofing).
- *Powerful and innovative Capabilities of control:* Stateful Inspection of scans and Trojan attacks: SPHINX uses a unique Stateful Inspection technology to discover if a user's station is attacked or analyzed by a foreign station on the Internet or from the LAN. This technology enables users to block any kind of hacking flow, not just TCP based attacks. IT also blocks any foreign IP, UDP, ARP communications and also non IP protocol based attacks (IPX, NetBEUI, etc.). Various kinds of actions like interactive warnings and monitor warnings are offered regarding these connections.
- Advanced Filtering Possibilities: An Advanced Mode allows expert users to manually add, edit and delete powerful filtering rules, for various non standards protocols and services. Users are able to specify time stamped rules with the option of generating logs and warnings.
- *Time Access Control:* With SPHINX, users can specify the exact time, date and also the duration of network connections, putting unwanted user sessions under strict control.
- *Multi-User Security Profiles:* SPHINX offers an option to define the appropriate security access policy for each individual user.
- *Multi-Devices Security Profiles:* SPHINX offers an option to define a complete security access policy for each individual user
- *Stealth Mode of Control:* It is possible to hide SPHINX's presence and control from a PC user by disguising SPHINX's program icon and shortcut.
- *Application and service transparency:* Biodata's SPHINX runs in the background, transparent to end users. SPHINX can interact smoothly an securely with other applications.

Installation of SPHINX

System Requirements

To use SPHINX the following technical requirements are needed

- Pentium CPU or better
- Windows 98, Windows NT, Windows 2000
- 32 MB RAM or more
- 5 MB free disk space
- CD-ROM-drive

Installation Process

To install SPHINX, the following steps must be carried out :

- Start the PC
- Insert the SPHINX CD-ROM
- Click "Install" and follow the instructions
  (If the start window does not appear automatically then execute **setup.exe** on the CD-ROM)
- SPHINX will guide you through the installation process
- Reboot the PC

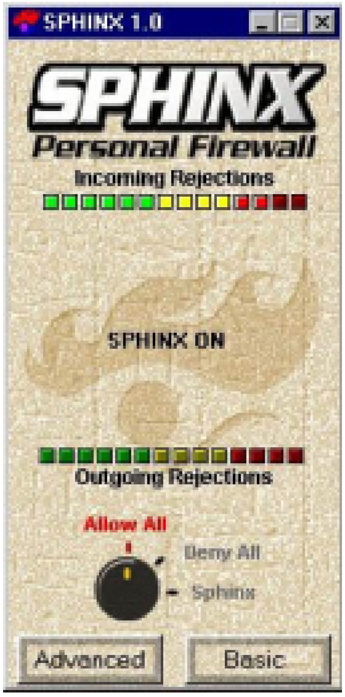
Attention: To avoid problems, it is necessary to remove the SPHINX driver first before disconnecting a network adapter or modem from the PC.

2

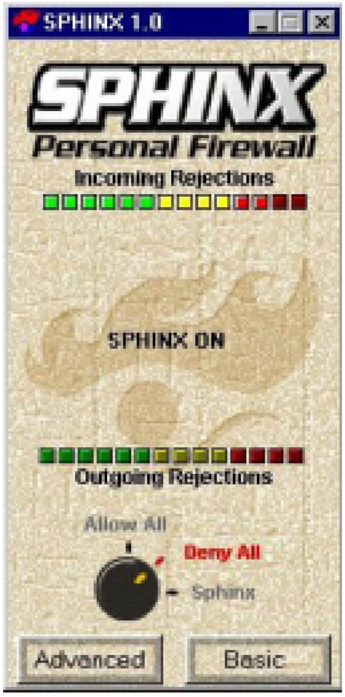
Start SPHINXing

2 Start SPHINXing

SPHINX can be started by clicking the SPHINX icon. By switching the main panel to "Allow All", you can check if the software has been successfully installed.



SPHINX runs in transparent mode now, and all packets are going through the filter engine without being checked. Now all services must work as before. If yes, switch to "Deny All" now.



The Sphinx is blocking all traffic now. No packet can be sent or received by the PC.

3

Making PCs Secure

3 Making PCs Secure

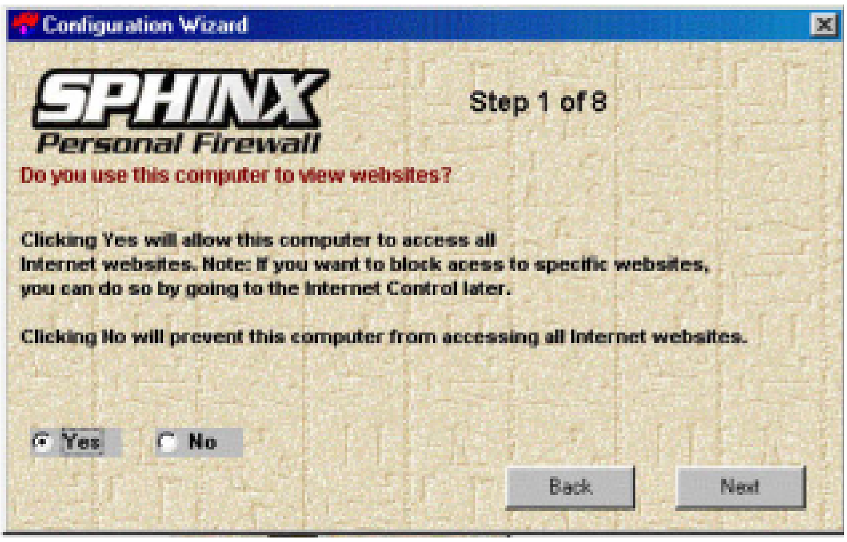
Normally, protection for a network should be warranted before that network is connected to the Internet. To protect a network a firewall should be installed. This firewall will control all packets, which come from the Internet and, depending on the configuration of the firewall, will decide whether to let the various packets through or not. The firewall also controls the outgoing packets from the internal network to the Internet. The firewall is thus protecting the machines in the internal network.

The same situation arises in the case of a standalone PC which is connected to the Internet. Normally there is no way of determining all incoming and outgoing traffic to or from a PC. Users cannot recognize attacks on their computer. However, if a "Trojan" is installed on the PC, hackers can get access to the machine, and with hacker tools like Netbus and Sub7 they have full control over any unprotected PC. That is why firewall security is not just an issue for large computer networks, but for every standalone PC.

Security Policy defines the actions which help to secure a network or a PC. This security policy also contains the list of the services which should be allowed by a firewall system. A firewall configuration should always be as narrow as possible. That means the configuration should just allow the services that are really needed. SPHINX offers capabilities to establish a security policy for the single PC, even for an administrator, who is not very familiar with security problems on the Internet. The best option for a newcomer to this field is to use the wizard.

The configuration wizard helps to generate the first configuration. The wizard will ask step by step questions to configure the specific services. Users can answer all these questions with a simple yes or no. By means of the easy to use configuration wizard users install an effective basic firewall configuration.

Step 1: Would you like to view websites?



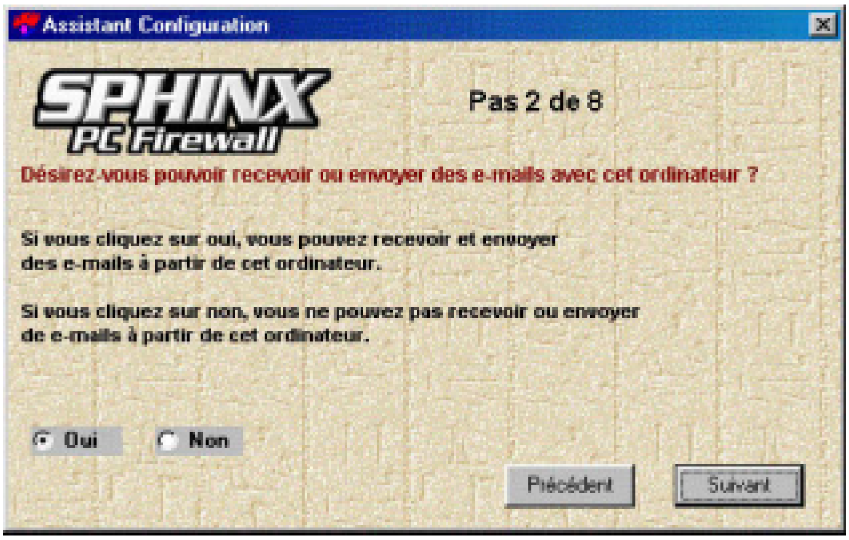
Do you use this computer to view websites?

Clicking Yes will allow this computer to access all Internet websites. Note: If you want to block acess to specific websites, you can do so by going to the Internet Control later.

Clicking No will prevent this computer from accessing all Internet websites.

By answering "Yes" you allow access to all websites from the Internet without any restriction. If your PC is also used by children and you therefore wish to control access to the Internet, you can click "Yes" here and specify the form of control to be exercised over the access to the Internet later in the menus "Advanced" and "Internet Control" (5.3, 5.4). For example: You have the opportunity of creating lists of websites which are strictly disallowed to be accessed (black lists). You also have the opportunity of defining a white list which includes all the websites which are allowed to be accessed: SPHINX will then block the access to all websites not specified in this white list.

Step 2: Would you like to send and receive e-mails?



Pas 2 de 8

Désirez-vous pouvoir recevoir ou envoyer des e-mails avec cet ordinateur ?

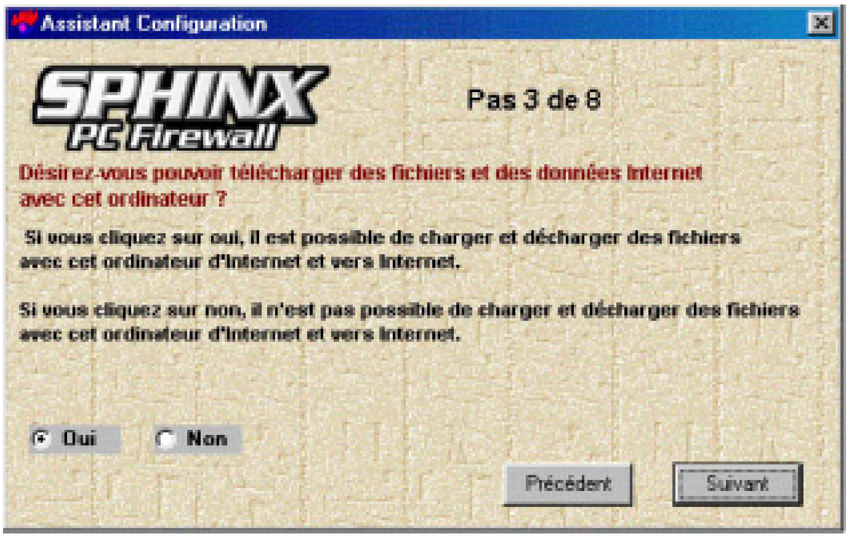
Si vous cliquez sur oui, vous pouvez recevoir et envoyer des e-mails à partir de cet ordinateur.

Si vous cliquez sur non, vous ne pouvez pas recevoir ou envoyer de e-mails à partir de cet ordinateur.

● Oui ○ Non

If you answer "Yes" you can send e-mails via SMTP (Simple Mail Transport Protocol) as well as receive them via POP3. E-Mails can then be sent to all servers on the Internet and also be received from all of them. Because of the speed of transmission this kind of electronic communication is very popular among the Internet users.

Step 3: Would you like to download files, pictures and data from the Internet?



Pas 3 de 8

Désirez-vous pouvoir télécharger des fichiers et des données Internet avec cet ordinateur ?

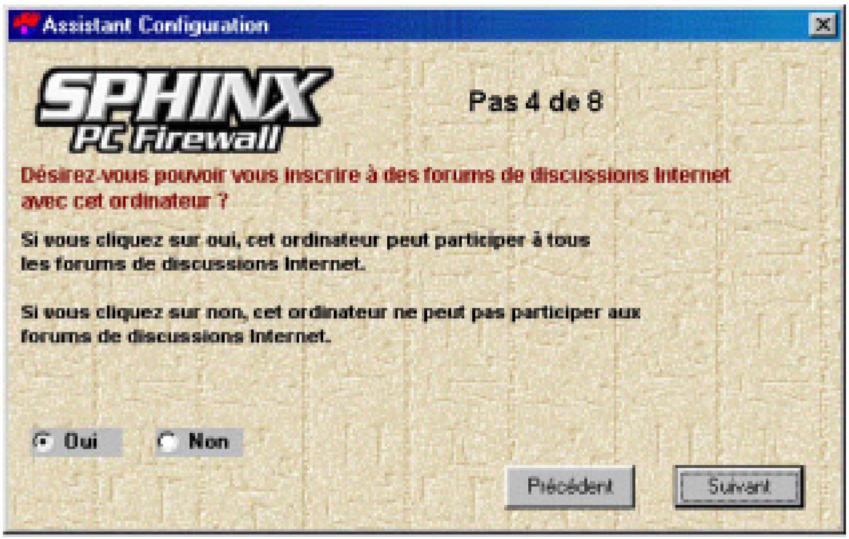
Si vous cliquez sur oui, il est possible de charger et décharger des fichiers avec cet ordinateur d'Internet et vers Internet.

Si vous cliquez sur non, il n'est pas possible de charger et décharger des fichiers avec cet ordinateur d'Internet et vers Internet.

● Oui ○ Non

By clicking "Yes" you allow your PC to download files, pictures and data of all kinds from the Internet. If you intend to download e.g. texts of websites on your PC or on disc, you should allow this option. This is also the case for pictures and complete programs like, for example, games which can often be downloaded from the Internet for free.

Step 4: Would you like to take part in news groups on the Internet?



Pas 4 de 8

Désirez-vous pouvoir vous inscrire à des forums de discussions Internet avec cet ordinateur ?

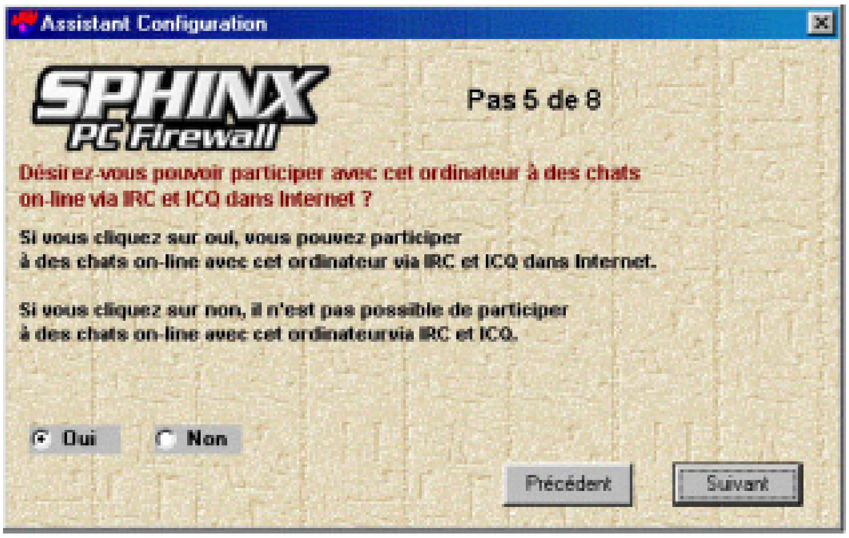
Si vous cliquez sur oui, cet ordinateur peut participer à tous les forums de discussions Internet.

Si vous cliquez sur non, cet ordinateur ne peut pas participer aux forums de discussions Internet.

◉ Oui ○ Non

News groups offer Internet users the opportunity of exchanging their views and experiences regarding various subjects. If you need e.g. advice for a special problem with your computer, news groups might offer you a solution to it. In order to read these messages or to send them to news groups, you need a so-called newsreader. Netscape offers you a standard newsreader within the installation of the webbrowser "Navigator". Of course, other newsreaders are also available.

Step 5: Would you like to chat on the Internet?



Pas 5 de 8

Désirez-vous pouvoir participer avec cet ordinateur à des chats on-line via IRC et ICQ dans Internet ?

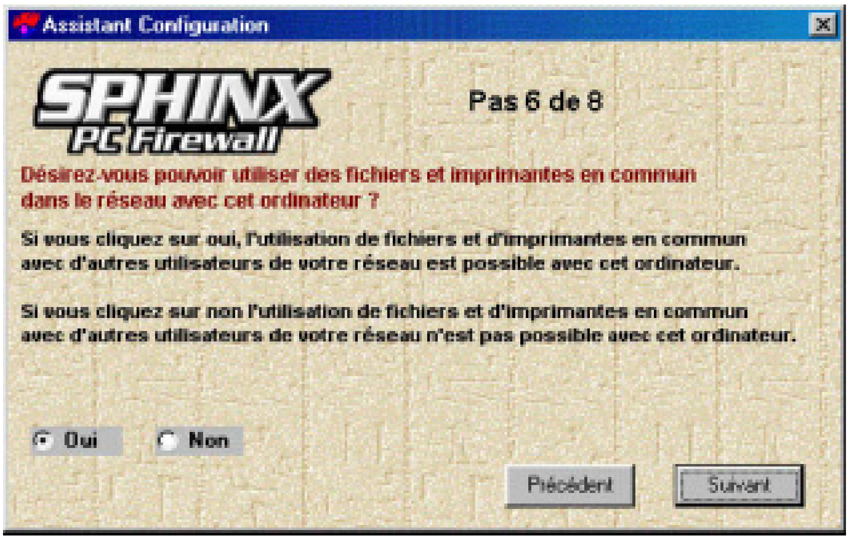
Si vous cliquez sur oui, vous pouvez participer à des chats on-line avec cet ordinateur via IRC et ICQ dans Internet.

Si vous cliquez sur non, il n'est pas possible de participer à des chats on-line avec cet ordinateurvia IRC et ICQ.

◉ Oui ○ Non

Chatting gives you the opportunity of simultaneously communicating with several other PC users via Internet. You first have to register at an adequate server which subsequently enables you to exchange messages. You will find a lot of chatrooms on the Internet which cover various topics and give you the opportunity of articulating your views.

Step 6: Would you like to share files and printers with other users in your network?



Désirez-vous pouvoir utiliser des fichiers et imprimantes en commun dans le réseau avec cet ordinateur ?

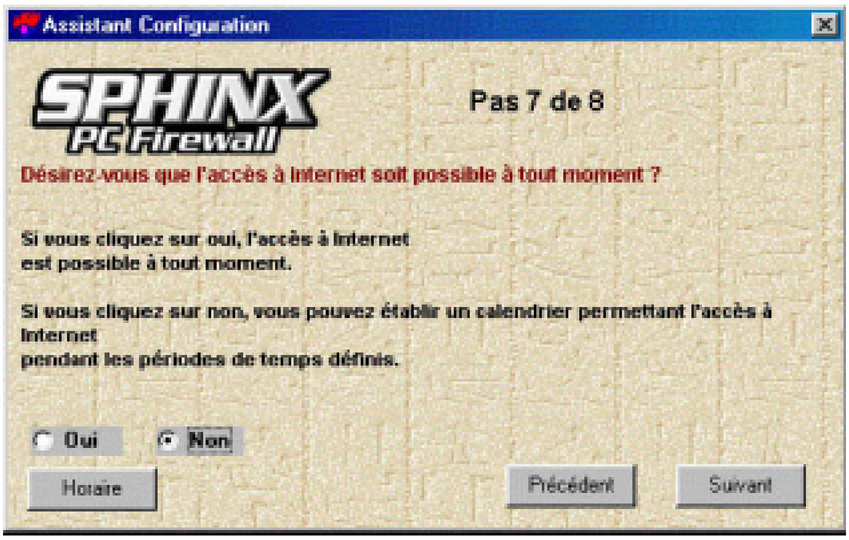
Si vous cliquez sur oui, l'utilisation de fichiers et d'imprimantes en commun avec d'autres utilisateurs de votre réseau est possible avec cet ordinateur.

Si vous cliquez sur non l'utilisation de fichiers et d'imprimantes en commun avec d'autres utilisateurs de votre réseau n'est pas possible avec cet ordinateur.

● Oui ○ Non

Printers connected to a single PC in a network can also be used by other members of the network. The access of other users to this printer must then be defined in the network configuration. If you use SPHINX on a PC with an installed modem or an ISDN card, that is: if your PC has no Ethernet connection, this function will probably not be necessary: In this case the printer is often directly connected to the PC so that printing orders will not be sent via the network.

Step 7: Would you like to have unlimited access to the Internet?



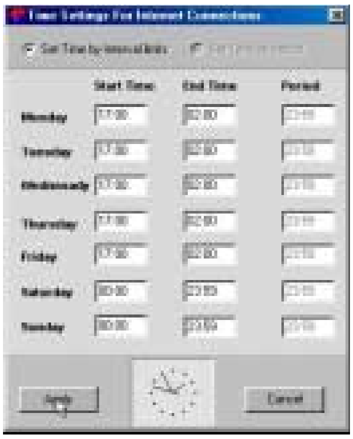
Désirez-vous que l'accès à Internet soit possible à tout moment ?

Si vous cliquez sur oui, l'accès à Internet
est possible à tout moment.

Si vous cliquez sur non, vous pouvez établir un calendrier permettant l'accès à
Internet
pendant les périodes de temps définis.

○ Oui ● Non

By answering "Yes" you allow permanent access to the Internet, not only for yourself but also for other users of this PC, e.g. children and employees. Clicking "No" will allow you to fill in the following time schedule:



Time Settings For Internet Connections

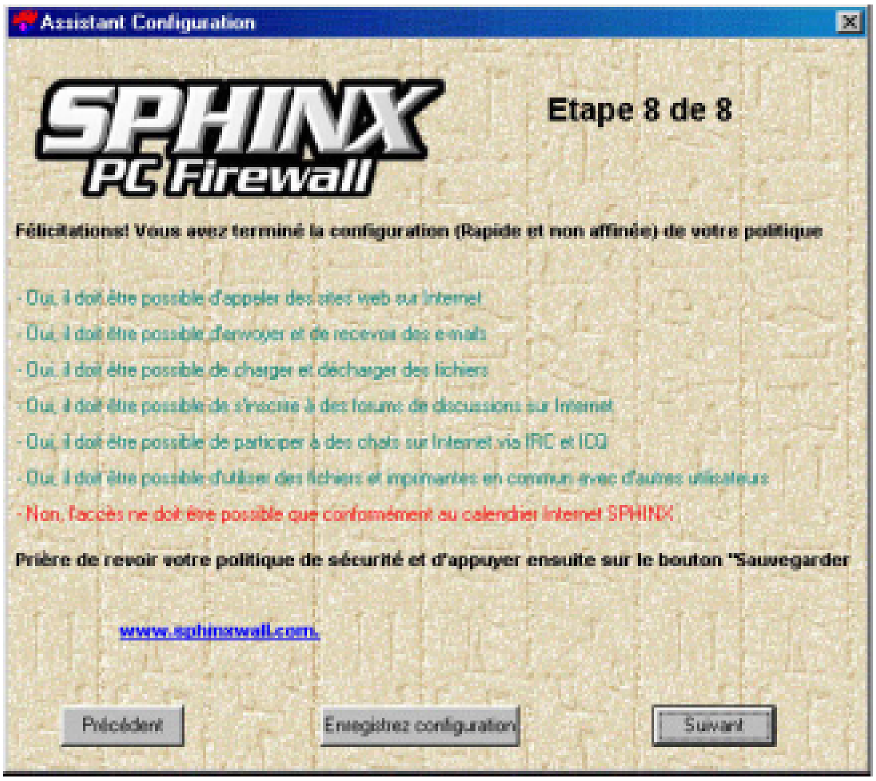
○ Set Time by interval limits ○ [illegible]

	Start Time	End Time	Period
Monday	17:30	02:00	23:59
Tuesday	17:30	02:00	23:59
Wednesday	17:30	02:00	23:59
Thursday	17:30	02:00	23:59
Friday	17:30	02:00	23:59
Saturday	00:00	23:59	23:59
Sunday	00:00	23:59	23:59

In the first two lines, you can define a start and an end date for the following time settings. If you want these time settings to be continued after the defined end date, you can of course re-define it and thus prolongue the settings as long as you wish. You can also change these settings whenever you want.

You can limit the access to the Internet either by interval limits or by a certain period, i.e. a set amount of time, for every day of the week. To define the interval limits you have to specify the start time and the end time between which the Internet should be accessible on the day in question. Would you like to limit the access to the internet to a certain daily amount of time, e.g. 2 hours, you have to turn to the column "Period". You then have to specify the period of use for the day in question. This function is very convenient, especially for parents who want to limit the daily use of the Internet by their children but cannot take care of it personally.

Step 8: Confirm SPHINX Security Policy



Etape 8 de 8

Félicitations! Vous avez terminé la configuration (Rapide et non affinée) de votre politique

- Oui, il doit être possible d'appeler des sites web sur Internet
- Oui, il doit être possible d'envoyer et de recevoir des e-mails
- Oui, il doit être possible de charger et décharger des fichiers
- Oui, il doit être possible de s'inscrire à des forums de discussions sur Internet
- Oui, il doit être possible de participer à des chats sur Internet via IRC et ICQ
- Oui, il doit être possible d'utiliser des fichiers et imprimantes en commun avec d'autres utilisateurs
- Non, l'accès ne doit être possible que conformément au calendrier Internet SPHINX

Prière de revoir votre politique de sécurité et d'appuyer ensuite sur le bouton "Sauvegarder

www.sphinxwall.com.

With this menu you can review your current SPHINX Security Policy and confirm or reconfigure it. In order to take full advantage of the numerous functions of SPHINX, you should later turn to the "Advanced Configuration" menu where you can specify your configuration settings.

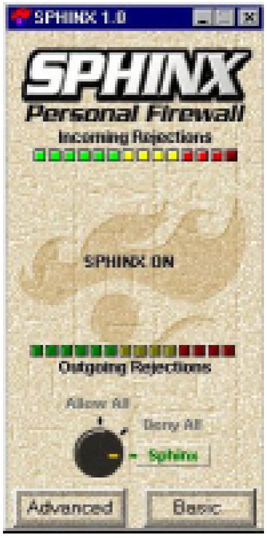
4

Exploring the SPHINX Mysteries

4 Exploring the SPHINX Mysteries...

4.1 Main Panel

After the installation of the SPHINX Graphical User Interface and the SPHINX filter engine, configuration can begin. Clicking the SPHINX icon will show the start menu:



The radio button in this panel enables users to rapidly switch the SPHINX firewall's running mode to the following options:

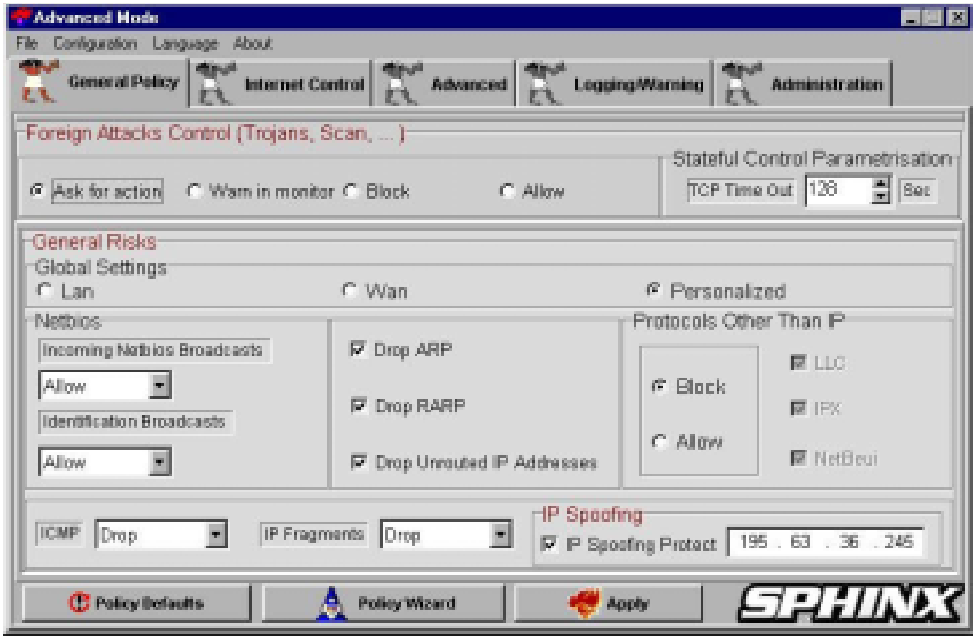
- **Allow All**: In this mode all network communication is permitted, without applying any controls. It is a pass through mode, in which the SPHINX control is disabled (this mode can be useful mainly for maintenance or for network audits by an audit tool). Please be careful when using this mode since in the "Allow All" mode NO protection is applied by SPHINX.
- **Deny All:** In this mode all network communications are blocked, without applying any finer control. It is a fully blocking mode, in which SPHINX prohibits any communication. This mode is used mainly for maintenance and troubleshooting. "Deny All" will virtually „pull the network plug", closing the door to any form of communication to the outside. This mode can be useful when you want to completely block access to your computer form the network.
- **SPHINX:** In the normal SPHINX mode, all the incoming/outgoing network flows are controlled, relatively to the policy specified by the active configuration of SPHINX. This is the usual mode of operation of SPHINX, permitting selective control on the communications to and from the user PC.
- The two progress bars show the rate (number of total packets / dropped packets) of denied incoming and outgoing network flow. When they become red, that means that the rate of dropped packets is becoming high. If the upper progress bar becomes red, it means that your station is subject to attacks or advertising web sites. If the lower progress bar becomes red, it means that a lot of attempts to access denied services from your station are ongoing, or that your browser is trying to send replies to cookies.

SPHINX offers two modes of configuration, depending on your needs and firewall expertise:

- **Basic Configuration:** This mode is suited for users that do not need a refined level of access control. It activates the basic configuration functions offered by SPHINX.
- **Advanced Configuration:** This mode is suited for users who need a high and refined level of control. It offers the full configuration functions provided by SPHINX. It is recommended to choose the basic level configuration first, and to subsequently go to the advanced mode once you have become familiar with the various firewall functions.

  When pressing one of these buttons, a popup menu leads you to the several configurations features of SPHINX.

4.2 Pull-Down Menues



Foreign Attacks Control (Trojans, Scan, ...)

● Ask for action ○ Warn in monitor ○ Block ○ Allow

Stateful Control Parametrisation

TCP Time Out 128 Sec

General Risks

Global Settings

○ Lan ○ Wan ● Personalized

Netbios

Incoming Netbios Broadcasts: Allow

Identification Broadcasts: Allow

☑ Drop ARP

☑ Drop RARP

☑ Drop Unrouted IP Addresses

Protocols Other Than IP

● Block ○ Allow

☑ LLC ☑ IPX ☑ NetBeui

ICMP: Drop

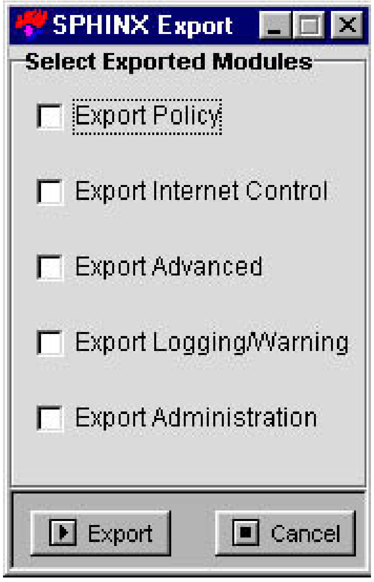
IP Fragments: Drop

IP Spoofing

☑ IP Spoofing Protect 195 . 63 . 36 . 245

4.2.1 File

Adding to the classical load / save you can export parts of the current loaded configuration or import configuration form other PCs. This can be useful when replicating partial control policies on several PCs. To open the Export window, just click "Export" under "File".



Select Exported Modules

□ Export Policy

□ Export Internet Control

□ Export Advanced

□ Export Logging/Warning

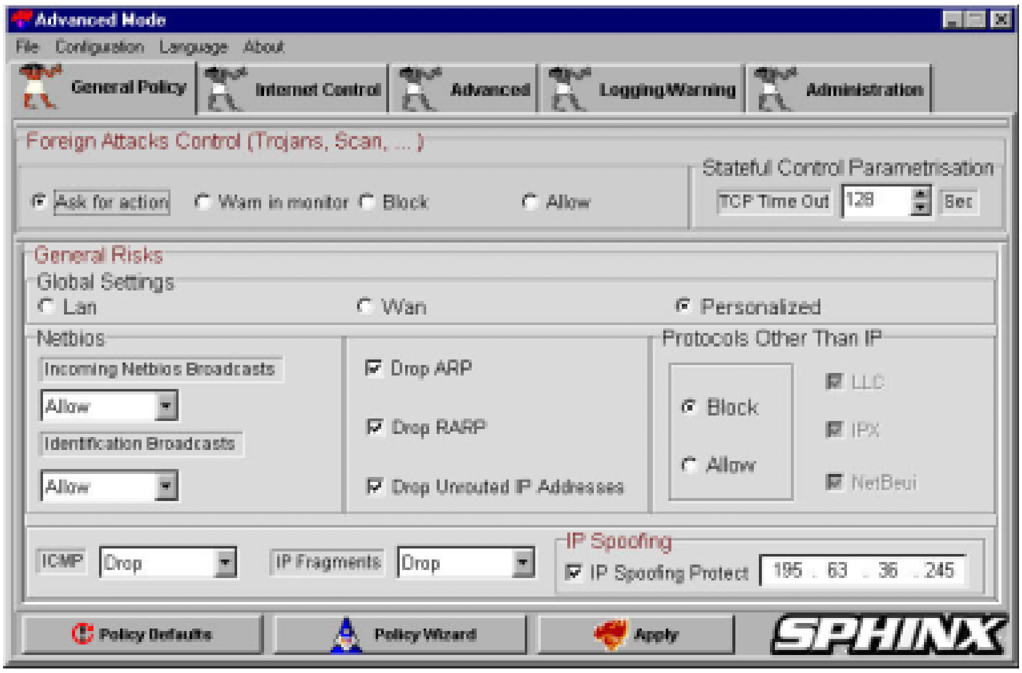
□ Export Administration

Select the configuration part which should be exported and click the export button to save it into a file. In the same way configurations can be imported from other PCs by clicking "Import"

4.2.2 Configuration

Every time you complete changes in the current configuration and have decided to apply it, you can do this by choosing the option <Apply> in <Configuration Menu>. The current configuration will then be immediately sent to the SPHINX driver. Due to security considerations, changes are not applied automatically. Push the "Apply" button once you have finished the firewall configuration. Apply-buttons are also available on every other panel like "General Policy" or "Internet Control".

4.3 General Policy Panel



Foreign Attacks Control (Trojans, Scan, ...)

● Ask for action ○ Warn in monitor ○ Block ○ Allow

Stateful Control Parametrisation

TCP Time Out 128 Sec

General Risks

Global Settings

○ Lan ○ Wan ● Personalized

Netbios

Incoming Netbios Broadcasts: Allow

Identification Broadcasts: Allow

☑ Drop ARP

☑ Drop RARP

☑ Drop Unrouted IP Addresses

Protocols Other Than IP

● Block ○ Allow

☑ LLC ☑ IPX ☑ NetBeui

ICMP: Drop

IP Fragments: Drop

IP Spoofing

☑ IP Spoofing Protect 195 . 63 . 36 . 245

Foreign Attacks (Scans, Trojans)

SPHINX uses an exclusive Stateful Inspection technology to discover if your PC is being attacked or analyzed from a foreign station on the Internet or from your LAN. This technology allows to block any kind hacking attempts, not just TCP based attacks. IT also blocks any foreign IP, UDP, ARP communication and non IP protocols based attacks (IPX, NetBEUI).

Allow: When this option is activated, SPHINX is neutral and does not stop any communication. Be careful when you activate this option, since in this mode foreign attacks and scans are not blocked.

BLOCK: This option activates the Stateful Inspection Technic of SPHINX, but does not put any warn messages out.

Warn in monitor: This option enables you to block foreign connections and also to be warned in the Warning Monitor about hacker attacks. When SPHINX detects foreign connection attempts, it will raise a warning in the <Foreign Connection Attempts> panel of the Warning Monitor (see Warning Monitor). For deeper analysis, you can then block attacks and examine them in the Warning Monitor.

Ask for Action: This option enables you to block foreign connections and also to be warned interactively, by means of an interactive pop up menu regarding such attacks. This pop up menu will inform you also about the probable tools of attack. To offer full flexibility, users are allowed to interactively decide about the action to take (Block/Allow). They are offered this possibility in case an expert user wants further observation and audit of an attack and some network audit (passive attacks) tools are used in your LAN environment.

Stateful Control Parametrisation: This is a basic parameter of SPHINX Stateful Inspection Technology: Idle time after which the connection you have established to a remote server will be finished and any packet coming from this server will be also considered as a foreign connection attempt. This value enables the user to calibrate the Stateful Inspection Technology in special cases of very slow WAN connections. It should be increased if you have a very slow network connection (when some legitimate connections will time out).

General Risks Protection

Global Settings:

LAN: When this box is activated, SPHINX will automatically set the necessary requirements for communication protocols in local area networks. SPHINX will allow

- ARP, RARP and "Unrouted IP Addresses"
- NetBIOS broadcasts
- Identification broadcasts
- ICMP protocol
- IPX, LLC and NetBeui

and will drop fragmented packets.

These are settings which are absolutely needed for a use in a Local Area Network (i.e. Ethernet) are fixed in the configuration. For examble ARP packets are necessary for the work in a Local Area network, it makes no sense to drop these packets with the Sphinx. Also Netbios broadcasts will be allowed if Sphinx is used in a LAN. Netbios broadcasts are needed for the use of a Windows Network. Netbios can be used to exchange files between two Windows PC's. The Ping, which is a tool to check wether or not a Computer is available in the network, is using the ICMP protocol. That's why ICMP is allowed for the use in LANs. Fragments are dropped, because they can be a security hole. Many attacks have been done with fragmented packets in the past.

WAN: When this box is activated, SPHINX will automatically set the necessary requirements for communication protocols in wide area networks. SPHINX will drop:

- NetBIOS broadcasts
- Identification broadcasts
- IPX, LLC and Netbeui
- ICMP
- ARP, RARP and "Unrouted IP Adresses"

The Spoofing Protection will be activated.

The ARP packets do not have any functionality, that's why they are not necessary. Also Netbios is not necessary for the use of a WAN connection.

Personalized: When this checkbox is activated, the Administrator can change the Parameters in this panel as he wants. All selectable functions under "General Risks" in the "General Policy"-panel can be changed, independent from the used interface.
The following options enable you to specify the control of types and forms of communications normally used in attacks.

Drop ARP/RARP:

It is HIGLHY recommended to allow ARP flows, if you are connected to a LAN. Otherwise you will prevent your computer from accessing the LAN. RARP is not necessary in most cases.

DROP UNROUTED IP ADDRESSES

It is recommended to activate this option and drop unrouted IP addresses. Some attacks are based on these addresses. Unless you are using the unrouted IP addresses for your local network area, like in a LAN for instance, please ask your security administrator about which decision to make.

ICMP

It is recommended to block ICMP packets, if you have a modem connection to the Internet, since information and actions related to this protocol like "Smurf Attacks" or DoS (Denial of Service) attacks jeopardize the security of your computer and also of other PCs. If you are connected to a LAN, please ask your security administrator about which decision to make, since this protocol can be useful at this network level.

IP FRAGMENTS

It is recommended to activate this option and drop fragmented IP packets. Some attacks are based on security holes in the process of the reassembly of (IP) communication messages.

IP SPOOFING Protect

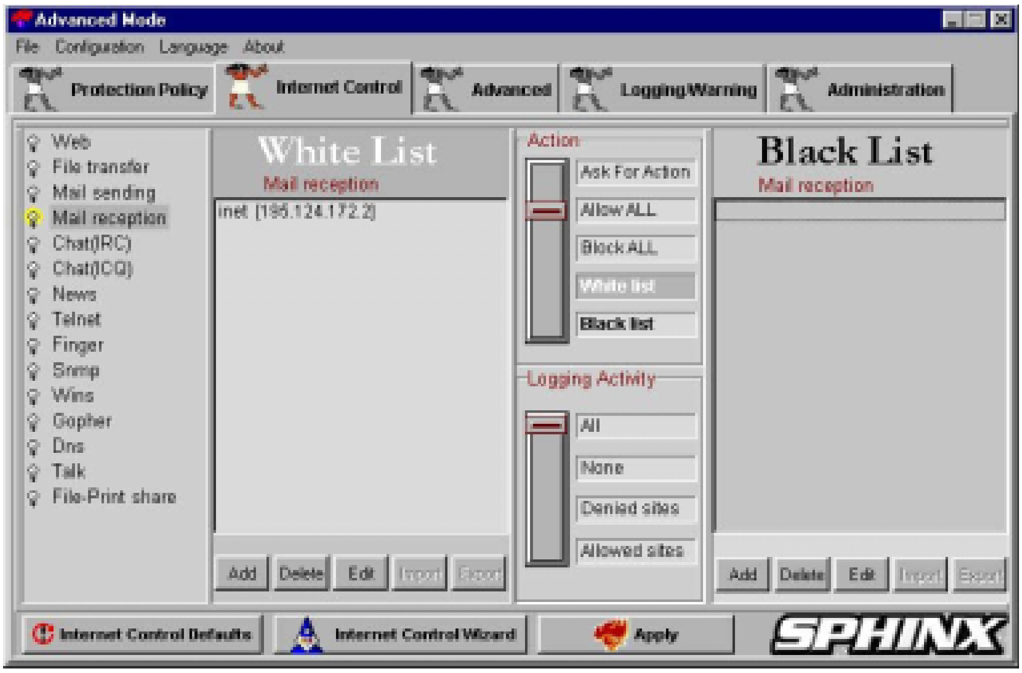
It is recommended to activate this option to make sure that your computer will not be the source of attacks on other stations. By using tools that change the source (IP) address of your usual communication (IP Spoofing) it is possible to hack other computers (see more details about those kinds of attacks in the help file of this wizard). You have to be aware that a little overhead will be occasioned by choosing this option.

This option is useful in LAN environments since it enables you to prohibit users from changing assigned IP addresses. If users change an IP address without the authorization of the administrator, they will not be allowed to communicate over the LAN. The use of another station's IP address can cause trouble in some LAN environments and can also be purposely used to initiate IP Spoofing attacks.

Protocols Other Than IP (IPX/SPX,NetBEUI)

If you only use the Internet and if your station is not part of a Novell local area network and if you are not running or using an application built on NetBEUI (an IBM specific protocol used in some Microsoft environments), it is recommended to block communication using protocols other than IP protocols. If you are connected to a LAN, please ask your security administrator about which decision to make.

4.4 Internet Control



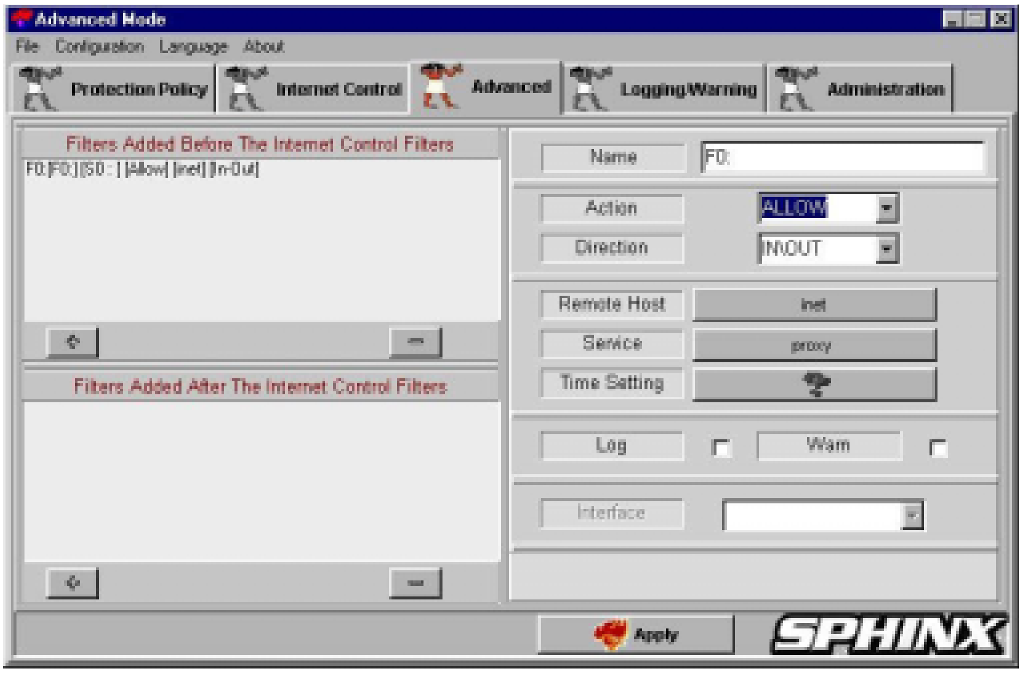
inet [195.124.172.2]

This panel enables users to add control rules to a variety of Internet services including Web, FTP, sending mail, receiving mail, chat, IRC and more. By default all services are allowed. Select the sub panel of the Internet service you want to introduce and choose the kind of control and logging you want apply:

Action
Ask For Action: Choosing this option enables you to be asked (interactively or in the Monitor) whether you want to access a site with a selected Internet service like FTP or IRC
Allow All: This option allows access to ALL sites
Block All: This option blocks access to ALL sites.
Black List / White List: SPHINX allows you to choose two kinds of access control strategies:
Black List: This mode will allow access to all OTHER sites not specified in the black list window. The sites inserted in the black list will be blocked.
White List: This mode will allow EXCLUSIVE access to the sites specified in the white list windows. All other sites will be blocked.

The Internet Control functionality provides you with a set of effective mechanisms for parental and academic control. Simply use the "Add", "Delete" and "Edit" buttons to set up and update your black and white lists. You can specify sites by giving their URL (Internet sites) or IP addresses (LAN). It is also possible to import and export complete URL lists. The Internet Control panel enables you to set up a Black List of suspicious URLs with racial, pornographic or dangerous contents. Alternatively, you can also block all URLs and allow only particular sites listed in the White List.

4.5 Advanced Configuration

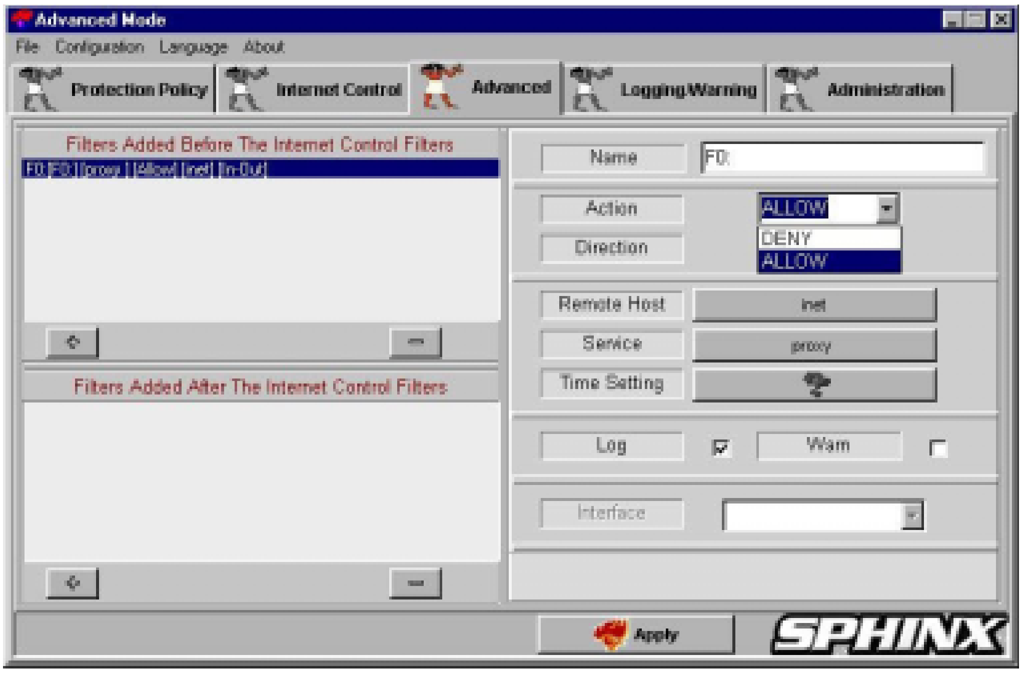


F0:[F0:] [SD:] [Allow] [inet] [In-Out]

Name: F0:
Action: ALLOW
Direction: IN\OUT
Remote Host: inet
Service: proxy
Log □ Warn □

This menu is designed for users who have a good understanding of protocols and filtering rules. Offering the power of a professional firewall, SPHINX features extended configuration possibilities to control any kind of communication. You are allowed to define your proper network services and to generate filters which can be applied from the Internet Control Panel. The selected filters can be set to specific dates and times or for specific session period. This enables you to control how much time users can access services.

To allow specific services the following steps need to be taken:
The SPHINX filter table uses the "first match principle" If a network packet is received by the PC, SPHINX checks the filter table from top to bottom. This means that the order of filter lines is extremely important. If, for instance, HTTP in the "Filters added before the Internet Control Filters" window is denied in all directions, HTTP will not work, because it is blocked before the Internet Control filters. To start the process just click the "+" button and the following window will appear:


Advanced Mode
File Configuration Language About
Protection Policy
Internet Control
Advanced
Logging Warning
Administration
Filters Added Before The Internet Control Filters
Filters Added After The Internet Control Filters
Apply
SPHINX

F0:|F0:||proxy||Allow||inet||In-Out|

Name: F0:

Action: ALLOW (DENY / ALLOW)

Direction

Remote Host: inet

Service: proxy

Time Setting

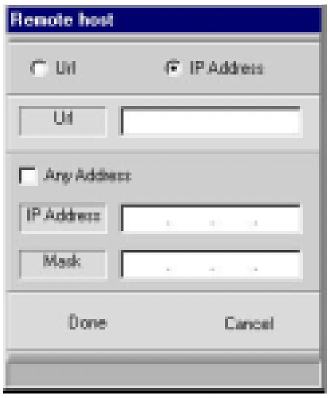
Log ☑ Warn □

Interface

Name: Each filter line has its own name.

Action: Clicking on the pull down arrow opens the pull down action menu
The user selects whether to allow or deny services or protocols.

Remote Host: Clicking on the question mark under "Remote Host" opens the following panel:



○ Url ● IP Address

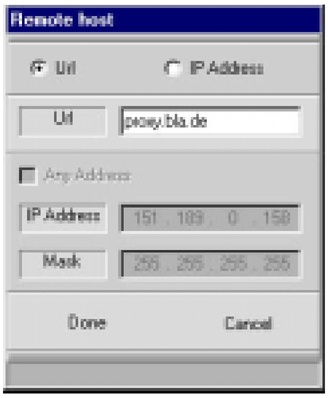
Url:

□ Any Address

IP Address: . . .

Mask: . . .

Users have the option to define the remote host to which this service should be allowed or denied. This can be done by defining the URL or IP Address of the Remote Host. In terms of using URL, the Domain Name service must be already allowed. In terms of IP addresses, there are some more possibilities which can be used. If "Any address" is checked, the defined service will be allowed or denied to any address, which means to the whole Internet.



● Url ○ IP Address

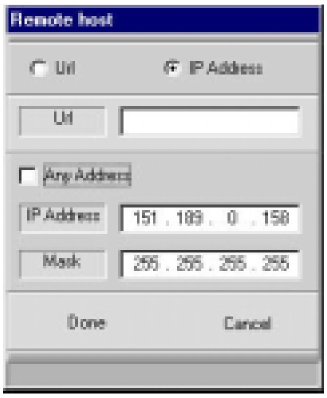
Url: proxy.bla.de

□ Any Address

IP Address: 151 . 189 . 0 . 158

Mask: 255 . 255 . 255 . 255

It is possible to use a specific IP address, a whole network or sub network which is defined by the network mask. In the case of a single host the network mask must be set to 255.255.255.255.



Remote host

○ Url ● IP Address

Url

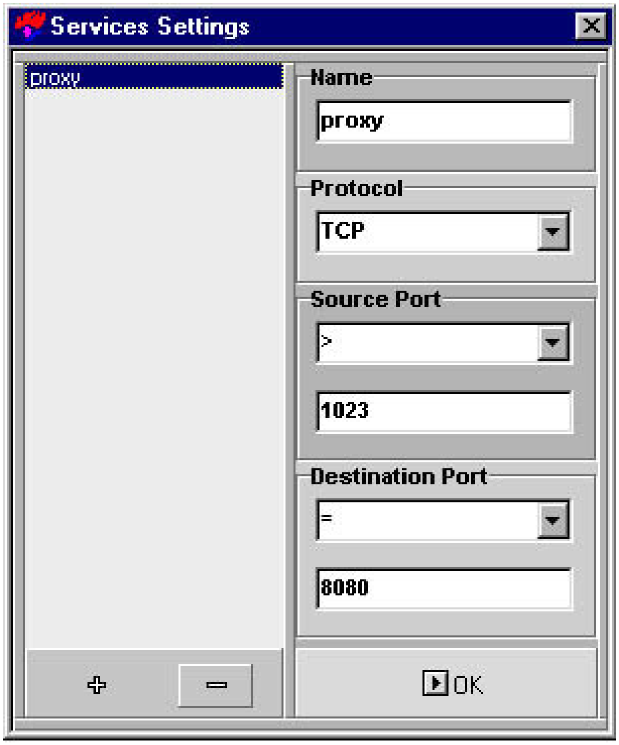
□ Any Address

IP Address 151 . 189 . 0 . 158

Mask 255 . 255 . 255 . 255

In this case, just one IP address is selected. The service in this filter line will be allowed or denied just to the IP address 151.189.0.158.

Clicking on the "Service" button opens the following window



Services Settings

proxy

Name: proxy

Protocol: TCP

Source Port: >

1023

Destination Port: =

8080

The "name" button defines the name of the service. Clicking on the pull down arrow opens the protocol pull down menu. The following protocols can be selected: IP, TCP, UDP, FRAGMENT, ICMP.

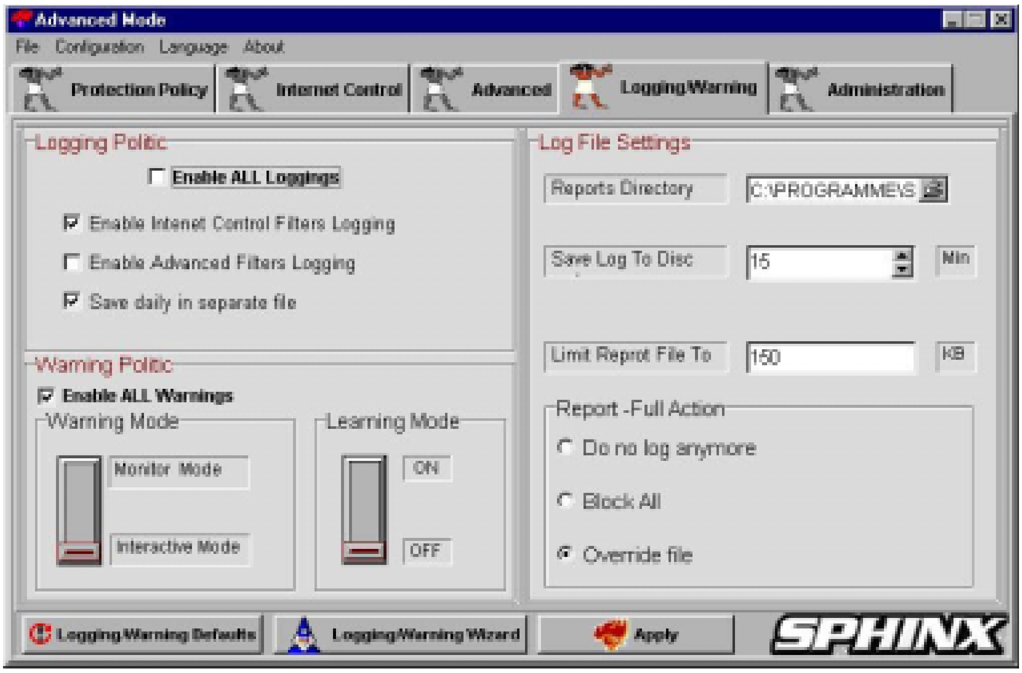
Logging Activity

For each service you have various logging options:

- ALL : All activities will be logged.
- Denied : Only access attempts to blocked sites will be logged.
- Allowed : Only access attempts to allowed sites will be logged.

4.6 Logging/Warning Panel

This panel enables users to configure different logging and warning policies. It enables users to restrict logging and warning by default, even if specified as activate in the various SPHINX menus.



☐ Enable ALL Loggings

☑ Enable Intenet Control Filters Logging

☐ Enable Advanced Filters Logging

☑ Save daily in separate file

☑ Enable ALL Warnings

Reports Directory C:\PROGRAMME\S

Save Log To Disc 15 Min

Limit Reprot File To 150 KB

○ Do no log anymore

○ Block All

● Override file

General Warnings

This setting enables users to specify, if they wish to activate or deactivate the warning notices. They decide if they want to receive interactive pop up menus or to automatically direct the warnings to the Warning Monitor.

1. Enable ALL Warning : If you uncheck this checkbox, you will not receive warnings from SPHINX.
2. Monitor Mode / Interactive Mode: When switched to interactive mode, pop up menus will inform you about warning messages, non defined flows and foreign connections attempts. This option is automatically set to the Monitor Mode, when SPHINX is selected to operate in Stealth Mode (< administrator> panel, see below) in which SPHINX operates in the background.

Learning Mode

This functionality offered by SPHINX enables you to interactively construct your control rules. For any flow that is not explicitly specified in your control policy, SPHINX will permit you to decide interactively or subsequently (<Warning Monitor>) about incorporating a control on such communication. This functionality enables you to progressively build your filtering database in an learning mode of operation.

If you are in <Monitor Mode> (Logging/Warning Panel), the Logging Monitor will inform you about each communication for which you have not specified an explicit filtering rule. It is then possible to click on such warnings and you will be prompted (with the same kind of popup menu) to decide. It is preferable to select this last mode, if you want to avoid repeated starts of popup menus.

General Logging

This setting will enable you to specify your GENERAL logging policies:

1. Enable Internet Control Filter Logging : If you check this checkbox, all Internet service activities like FTP or IRC will be logged. If unchecked, no logging will be done.
2. Enable Advanced Filters Logging : If you check this checkbox, all individual filters for which you requested logging will be logged. If unchecked, no logging will be made.
3. Save Daily in a Separate File: This option enables you to specify that logging is stored in a new file each day of the week or in a common file elsewhere.

Log File Settings

In order to provide users with an explicit control on the logging process, various functions are offered by this sub panel to protect them against attacks.

Limit Report File To: Specify maximum size for log file.

When Report Full: Specify which action to take when logging file is full.

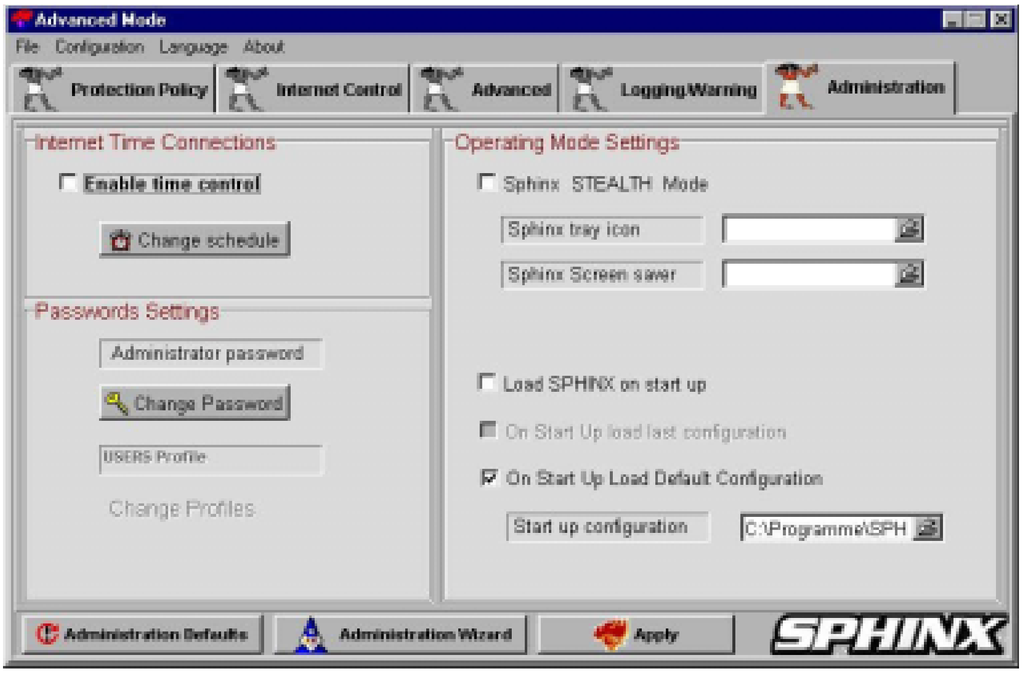
Overwrite File: The previous Logs will be erased and a new log file is created. This event will appear in the logging monitor under the panel <System Warnings>.

Block All Mode: SPHINX will block all communication and no longer perform logging activities.

Do Not Log Anymore: By default SPHINX will control data traffic, but without logging.

Save Log To Disk: Especially on slower PCs, storing data on disk can delay ongoing activities. SPHINX allows you to specify the intervals of time when the log files will be stored on disk. In between these periods, log files are only stored to main memory.

4.7 Administration Panel



☐ Enable time control

☐ Sphinx STEALTH Mode

☐ Load SPHINX on start up

☐ On Start Up load last configuration

☑ On Start Up Load Default Configuration

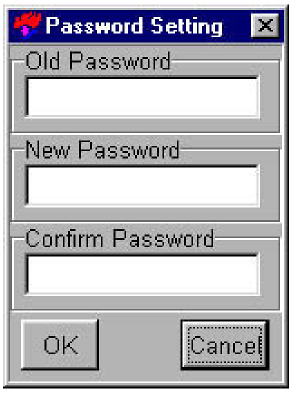
Start up configuration: C:\Programme\SPH

Internet Time Connections

This option enables you to control at what time your PC users can access the network when using Internet services.

Password settings

Clicking "Change Password" opens the following Pop-Up window:



The SPHINX password can be changed by entering the old and the new password.

Operating mode settings

SPHINX Stealth Mode :

SPHINX can operate in Stealth Mode, with users unaware of its presence, and so carry out control and activity logging. Selecting this option is useful to audit the activities on a PC connected to the network without user awareness. To enable this mode and hide from users who recognize the SPHINX standard icon and will detect its presence it is recommended to change the standard SPHINX icon and choose another one from the list of available icons on your PC and another prompt screen, rather than the usual SPHINX prompt screen.

IMPORTANT: To get the SPHINX login prompt, CTRL and Space key must be pressed together. The SPHINX password can be entered then, to get into SPHINX configuration mode.

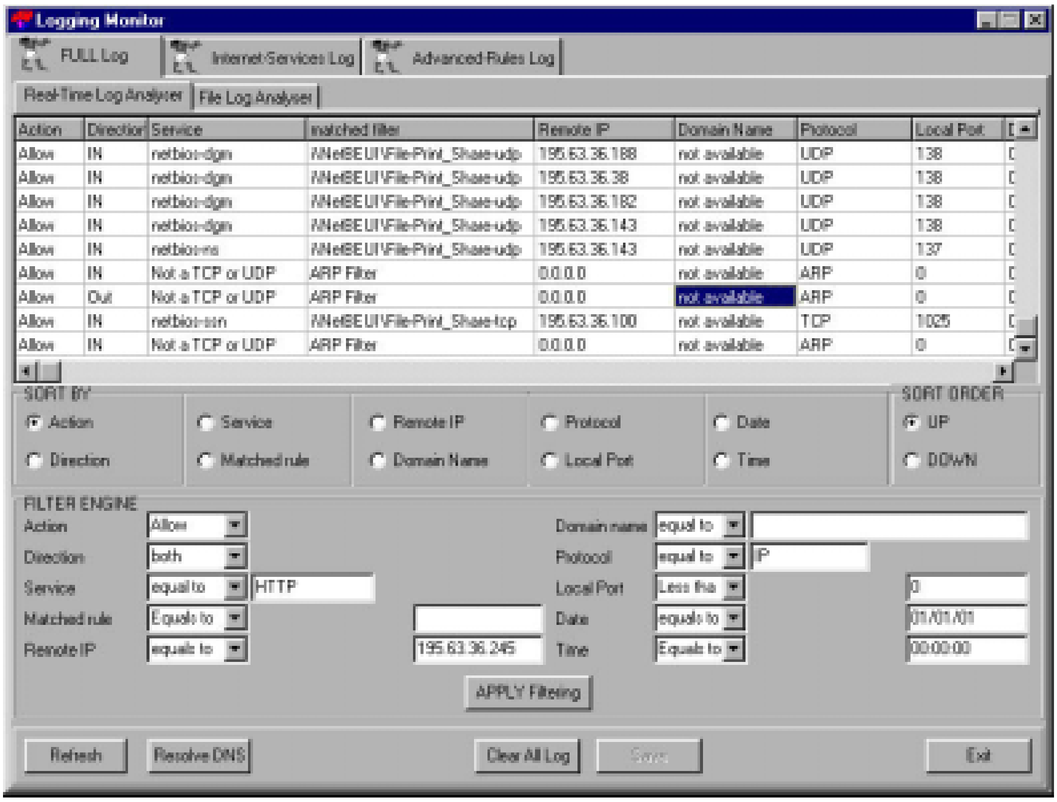
Always load last configuration

This option enables users to automatically load and activate the last loaded configuration (previous session).

4.8 Logging Monitor

The Logging Monitor offers three sub panels:

1. Internet-Services Log: Log files generated only by the Internet control policy <Internet control panel> sorted by services
2. Advanced Rules Log: Log files generated from the rules related to the <advanced control> panel.
3. Full Log Panel: All the registered log events will be shown in this panel. The previous panels permit selective examination of the log files (Internet control/advanced), but in this panel you can find the exact occurrence sequence of those selective logs (Internet Control/Advanced).



Action	Direction	Service	matched filter	Remote IP	Domain Name	Protocol	Local Port
Allow	IN	netbios-dgm	\NetBEUI\File-Print_Share-udp	195.63.36.188	not available	UDP	138
Allow	IN	netbios-dgm	\NetBEUI\File-Print_Share-udp	195.63.36.38	not available	UDP	138
Allow	IN	netbios-dgm	\NetBEUI\File-Print_Share-udp	195.63.36.182	not available	UDP	138
Allow	IN	netbios-dgm	\NetBEUI\File-Print_Share-udp	195.63.36.143	not available	UDP	138
Allow	IN	netbios-ns	\NetBEUI\File-Print_Share-udp	195.63.36.143	not available	UDP	137
Allow	IN	Not a TCP or UDP	ARP Filter	0.0.0.0	not available	ARP	0
Allow	Out	Not a TCP or UDP	ARP Filter	0.0.0.0	not available	ARP	0
Allow	IN	netbios-ssn	\NetBEUI\File-Print_Share-tcp	195.63.36.100	not available	TCP	1025
Allow	IN	Not a TCP or UDP	ARP Filter	0.0.0.0	not available	ARP	0

SORT BY

● Action ○ Service ○ Remote IP ○ Protocol ○ Date
○ Direction ○ Matched rule ○ Domain Name ○ Local Port ○ Time

SORT ORDER

● UP
○ DOWN

FILTER ENGINE

Action: Allow
Direction: both
Service: equal to HTTP
Matched rule: Equals to
Remote IP: equals to 195.63.36.245
Domain name: equal to
Protocol: equal to IP
Local Port: Less tha 0
Date: equals to 01/01/01
Time: Equals to 00:00:00

Real Time Log Analyzer

This panel shows you the logging of the current session in real time. For additional analysis, you can start sorting and filtering functionality (see below).

Log File Analyzer

This Panel enables you to load previously stored log files and to analyze them using sorting and filtering functionality.

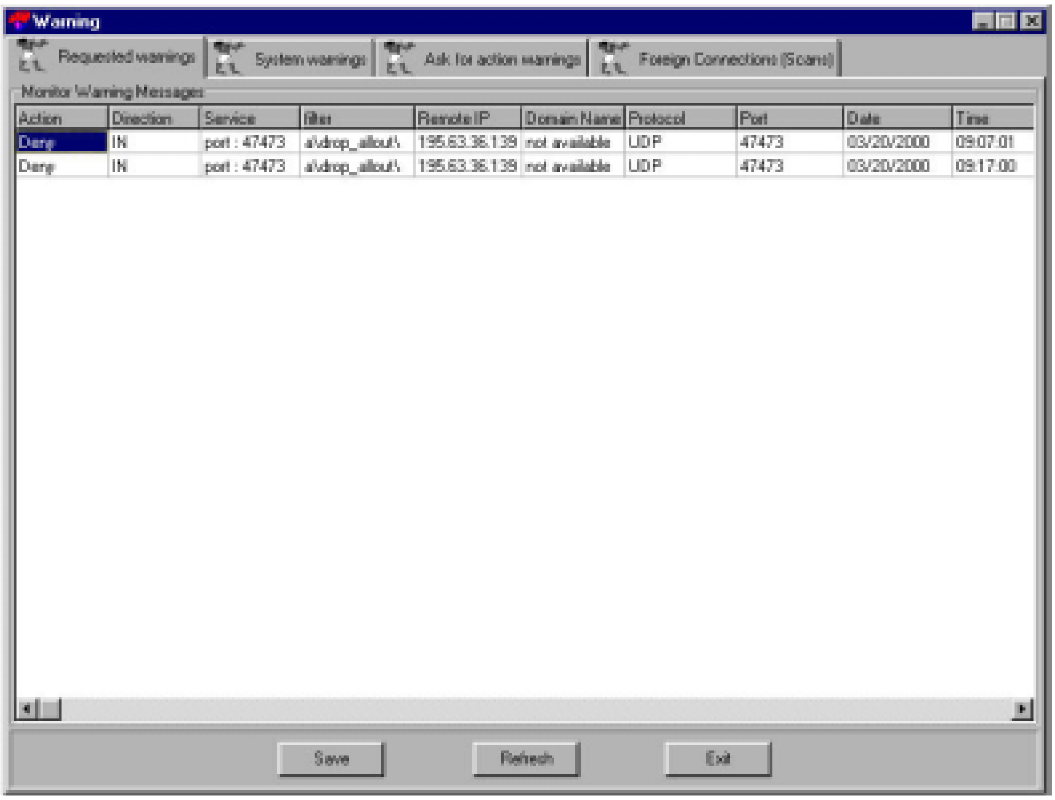
General Utilities

Resolve DNS: Listing URLs associated with the IP addresses registered in the log links, this option allows detailed examination of log files. This option will assume the existence of DNS server (or that you are connected to the Internet) and can be time consuming, if the amount of log files is large and your Internet connection is slow.
Refresh: In order to avoid the delay of user activities, SPHINX periodically retrieves logging data.
Clear ALL Logs: By Pushing this button, you erase all the present logging files. Please note that this will permanently erase all the present registered log files.
Print: Print the current logging file.

FILTERING and SORTING functions

SORT BY: This functionality will enable you to sort your log files in increasing or decreasing order(radio button SET ORDER). The sorting function concerns all the fields of the logging line (Action/Remote IP).
FILTER ENGINE: Rich and cumulative filtering functions are offered by SPHINX. They enable you to filter the logging lines on specific fields of the log files. You can apply PROGRESSIVE filters (next filter will be applied on the result of the previous filter and so on to allow the selective examination of the logging procedure.
To activate a configured filter, the "Apply Filtering" must be clicked.

4.9 Warning Monitor

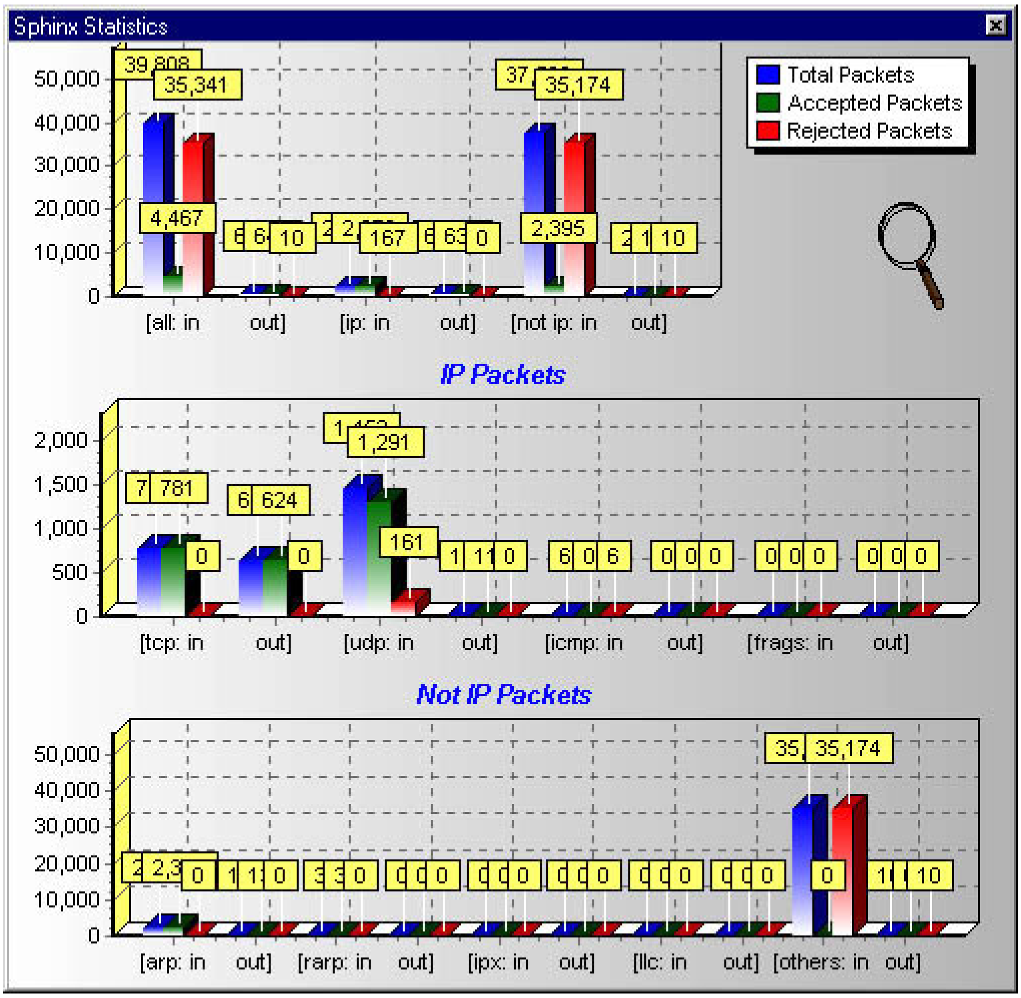


Action	Direction	Service	filter	Remote IP	Domain Name	Protocol	Port	Date	Time
Deny	IN	port : 47473	a\drop_allout\	195.63.36.139	not available	UDP	47473	03/20/2000	09:07:01
Deny	IN	port : 47473	a\drop_allout\	195.63.36.139	not available	UDP	47473	03/20/2000	09:17:00

The concept of Warning Monitor enables SPHINX administrators to register warning messages. When you choose to direct warning messages (learning mode and foreign connection attempts) to the logging monitor by selecting the monitor Mode in the panel <Logging/Warning>, these messages will be registered in the Warning Monitor. In this way, you can look at them later offline or during an auditing operation.

1. Requested Warnings: When logging service activities in the advances control mode, this menu will show the individual warnings.
2. System Warnings: This menu will report warnings related to the operation of SPHINX. The software will notify you whether logs files are full, disk space is limited or users have tried to log to SPHINX with invalid passwords. The menu will also list user actions like configuration loading or rules set in learning mode.
3. Ask For Action Warnings: If the learning mode is in use, here you can generate filter lines for different network data packets. Any data stream with undefined control rules is listed.
4. Foreign Connection Warnings: By selecting the "Block and Warn" or "Block and Ask for Action" buttons you can generate filter lines for the source packet host.

4.10 Statistics Panel



This function enables you to examine some statistics on the various network flows and report the dropping activity of SPHINX (number of dropped/allowed packets in both directions). This can be useful for immediately observing the rate of not allowed activity controlled by SPHINX.