Getting Started

German

SPHINX

PC Firewall

Inhaltsverzeichnis

GDieser Quick Guide ist eine Kurzanleitung, die es Ihnen erlauben soll, die erworbene Sphinx-Software zu installieren und eine Basiskonfiguration zu erstellen. Weitergehende Informationen finden Sie im Benutzerhandbuch, welches sowohl auf der CD gespeichert als auch auf der Webseite www.sphinxwall.com abrufbar ist.

1. Programm Installation

- Legen Sie die Sphinx–CD in das CD-Rom Laufwerk ein.
- Klicken Sie auf Installieren, wählen Sie die bevorzugte Sprache und folgen Sie den Anweisungen. Sollte das Installationsfenster nicht erscheinen, führen Sie die Datei Setup.exe auf der Sphinx-CD aus.

2. Starten von SPHINX

- Starten Sie die Sphinx durch wählen von "Start Programm Sphinx".
- Stellen Sie sicher, dass der Mode Knopf auf Allow All steht "Bild 1". Überprüfen Sie die Netzwerkverbindung. Gegebenenfalls müssen Sie dazu eine Internet-Verbindung aufbauen. Die Verbindung muss wie bis anhin funktionieren. Überprüfen Sie dies zum Beispiel durch aufrufen einer Seite wie: www.biodata.com.
- **VORSICHT:** Jeglicher Schutz von Sphinx ist noch nicht aktiviert.
- Hat die Verbindung funktioniert, stellen Sie den Mode Knopf nun auf Deny All. Es darf nun keine Verbindung mehr möglich sein. Überprüfen Sie dies zum Beispiel durch aufrufen einer Seite wie: www.sphinxwall.com.
- **WICHTIG:** Nur wenn Das Herstellen einer Verbindung nicht möglich ist, hat man die Sphinx einwandfrei installiert.

Bild 1

Bild 2

3. Konfiguration

Der einfachste Weg zu Ihrer persönlichen Konfiguration stellt der "Configurations-Wizard" dar. Starten Sie den "ConfigurationsWizard" unter Basic "Configurations-Wizard". Durch das Anlegen eines Passwortes haben Sie die Möglichkeit, die mit "Configurations-Wizard" erstellte Konfiguration gegen Veränderungen zu schützen. Bei der ersten Änderung bleibt das Feld "altes Passwort" leer.

Schritt 1 von 8

Durch beantworten dieser Frage, erlauben Sie ausgehende und eingehende Datenpakete von und zu Ihrem Browser wie Microsoft Internet Explorer, Netscape Navigator oder andere Webbrowser.

Schritt 2 von 8
Mit dieser Frage werden die für den Email-Verkehr benötigten Protokolle erlaubt, respektive verboten. Wenn Sie Emails empfangen und versenden wollen, müssen Sie diese Frage mit ja beantworten.

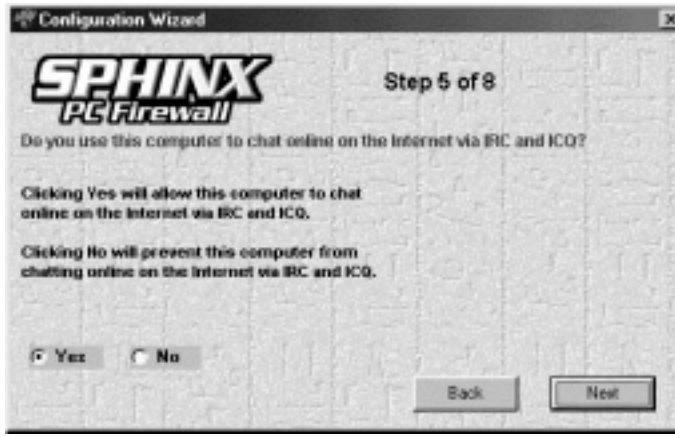
Schritt 3 von 8
Wenn Sie Dateien wie Bilder, Programme u.s.w. aus dem Netzwerk „Internet" laden wollen, müssen Sie diese Frage mit ja beantworten.

Schritt 4 von 8

Wählen Sie ja, wenn Sie an Newsgruppen im Internet teilnehmen wollen. Dabei handelt es sich um eine erweiterte Anwendung. Wenn Sie nicht Mitglied einer Newsgruppe sind, sperren Sie diesen Zugang indem Sie nein wählen.

Schritt 5 von 8

Wenn Sie sich auf einem Chat-Server anmelden wollen um mit anderen Internet-Benutzern auf einem Chat-Server zu kommunizieren, wählen Sie ja.

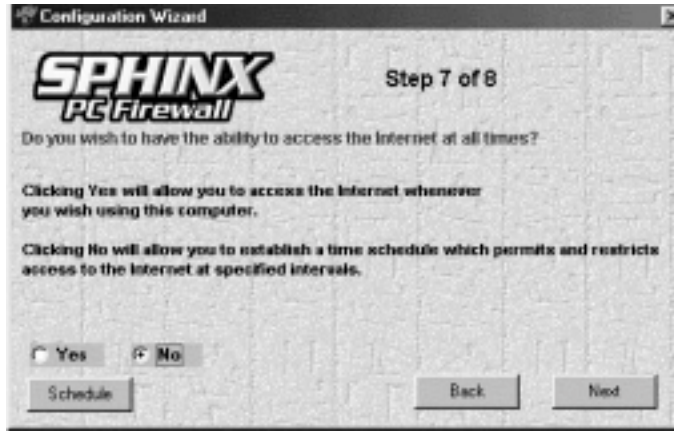


Schritt 6 von 8

Wenn Sie anderen Benutzern Daten oder ganze Verzeichnisse zur Verfügung stellen wollen, müssen Sie ja wählen. Auch das Drucken auf Ihren Drucker oder von Ihrem PC auf fremde Drucker, wird mit diesem Schritt erlaubt oder verboten. Wenn Sie sich über Modem ins Internet einwählen und über kein lokales Netzwerk verfügen, sollten Sie diesen Dienst auf alle Fälle durch das wählen von nein blockieren .

Schritt 7 von 8

Mit dieser Einstellung können Sie die zuvor getroffenen Einstellungen zeitlich begrenzen und ausserhalb dieser Zeit den Zugang zum Netzwerk, respektive Internet sperren. Zum Beispiel für die Zeit des Tages, in welcher Sie nicht Zuhause sind.



Mit der folgenden Einstellung würden Sie den Internet-Zugang von Montag bis Freitag, jeweils von 17:00 Uhr abends bis morgens um 02:00 Uhr, erlauben sowie samstags und sonntags den ganzen Tag.

Schritt 8 von 8

Schritt 9 zeigt Ihnen die erstellte Konfiguration nochmals in Form von Text an. Diese können Sie sogleich abspeichern. Anschliessend werden Sie nach dem Anklicken von "Weiter" aufgefordert, die Sphinx zu starten. Mit dem Bestätigen der Auswahl ist die Sphinx aktiv und schützt Ihren PC zuverlässig vor Angriffen.

Sie haben die Konfiguration Ihrer Sphinx Firewall erfolgreich abgeschlossen. **Wir Gratulieren!** Natürlich könne Sie diese Konfiguration noch verfeinern und Ihren Bedürfnissen anpassen. Informationen dazu finden Sie auf den folgenden Seiten und im Benutzerhandbuch.

4. Registration

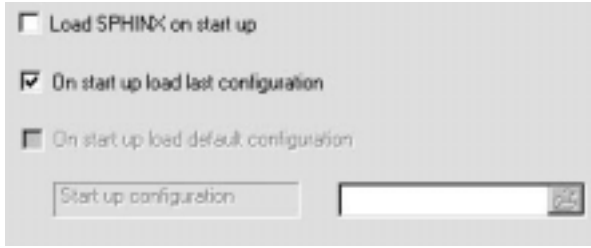
Registrieren Sie Ihre erworbene Sphinx-Software unter www.sphinxwall.com. Mit der Registrierung erhalten Sie eine neue Lizenznummer. Ändern Sie die Lizenznummer in Ihrer SPHINX um Sie jederzeit abrufbar zu haben. Nur mit einer solchen Lizenznummer sind Sie Supportberechtigt. Aus technischen Gründen beginnt die Supportberechtigung erst 2 Tage nach der Registrierung. Registrieren Sie sich deshalb umgehend, um in Problemfällen Wartezeiten zu vermeiden.

5. Wie verwalte ich meine Konfigurationen?

Damit Ihr Rechner sofort nach dem Hochfahren von Windows durch die SPHINX geschützt wird, sollte sie gleich mitgestartet werden. Dabei können Sie genau angeben, welche Konfiguration verwendet werden soll. Ebenso wichtig ist es, dass man eine erstellte Konfiguration speichern und später wieder zurückladen kann. Wer z.B. auf allen PC's in einer Netzwerkumgebung die SPHINX installiert hat, möchte natürlich nicht jedes Mal die Einstellungen neu vornehmen. Sie können einzelne Bereich, wie z.B. "Internet control", exportieren oder importieren. Alle Daten Ihrer Konfiguration werden in den Dateien verschlüsselt und sind somit optimal gesichert. Um den Zugriff auf die SPHINX zu sperren, können Sie noch zusätzlich ein Passwort vergeben. Es wird mit Hilfe des "Stealth"-Modus aktiviert, außerdem wird dadurch die SPHINX-Oberfläche beim Starten nicht geöffnet. Lediglich ein Icon in der Taskleiste von Windows zeigt an, dass ihr Rechner durch die SPHINX vor Angriffen geschützt wird.

So geben Sie die Startkonfiguration vor:

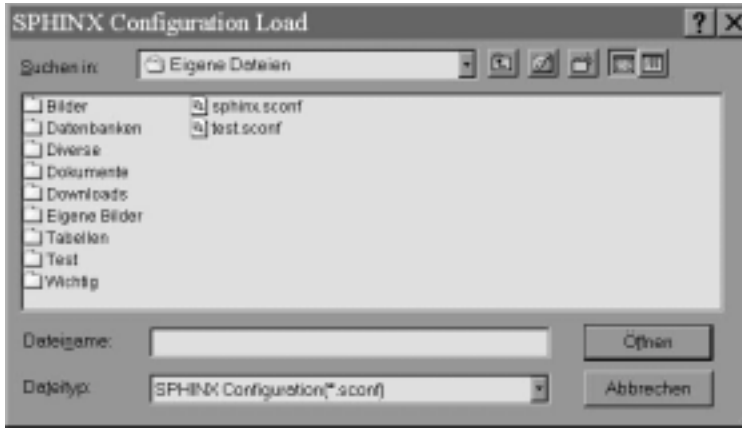
1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen Sie dann auf "Configuration"
3. Klicken Sie auf "Administration"
4. Aktivieren Sie die Option "Load SPHINX on start up"
5. Sie können zwischen folgenden Startkonfigurationen wählen:
   a. die zuletzt verwendete Konfiguration ("...load last configuration")
   b. Standardkonfiguration ("... load default configuration")
   c. eine Konfiguration vorgeben ("Start up configuration")



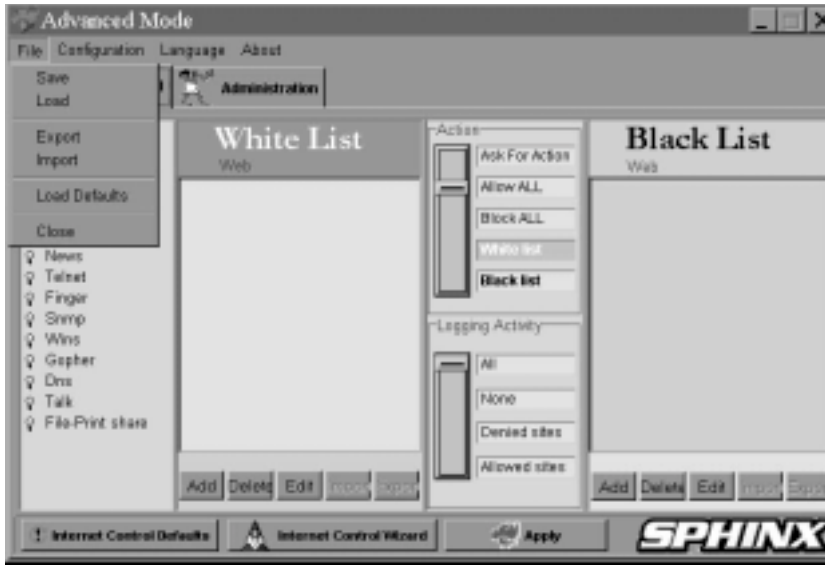
6. Klicken Sie "Apply" um die Konfiguration zu aktivieren.

So speichern/laden Sie eine Konfiguration:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Load/Save configuration"
4. Wählen Sie eine Konfiguration aus oder geben Sie direkt den Namen ein.

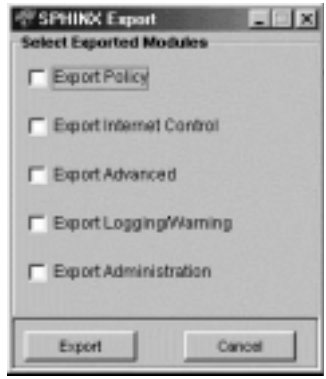


5. Klicken Sie auf "Öffnen/Speichern"
6. Wenn Sie eine Konfiguration geladen haben, klicken Sie "Apply" um die Konfiguration zu aktivieren
7. Hinweis: Sie können auch im Menü unter dem Punkt "File" die Option "Load/Save" auswählen:

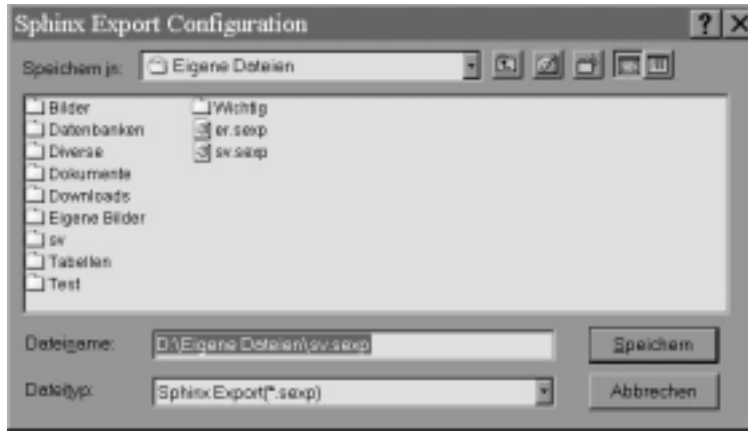


So exportieren/importieren Sie einen Bereich Ihrer Konfiguration (Modul):
Die ist vor allem dann nützlich, wenn Sie mehrere Benutzer einer Sphinx definieren wollen, die teilweise die gleiche Konfiguration verwenden.

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Im Menü unter dem Punkt "File" die Option "Export/Import" auswählen
5. Klicken Sie auf das entsprechende Modul, welches Sie exportieren/importieren wollen:



6. Wählen Sie ein Datei aus oder geben Sie direkt den Namen ein:

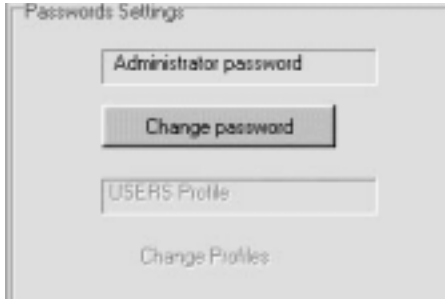


7. Klicken Sie auf "Speichern/Öffnen"
8. Wenn Sie ein Modul importiert haben, klicken Sie "Apply" um die Konfiguration zu aktivieren

So ändern Sie das Passwort:

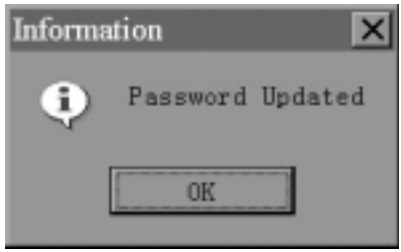
Beim ersten Wechsel bleibt das Feld altes Passwort leer.

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Administration"
4. Unter der Option "Passwords Settings" klicken Sie auf "Change Password":



5. Geben Sie nun Ihr altes Passwort ein, danach zweimal Ihr Neues:

6. Haben Sie es zweimal richtig eingegeben erscheint dieses Fenster:



7. Hinweis: Das Passwort bezieht sich auf die SPHINX und nicht auf die Konfiguration d.h., wird eine neue Konfiguration geladen, bleibt das Passwort gleich.

6. Wie konfiguriere ich die Internet-Dienste?

Die Internet-Dienste können leicht auf vier verschiedene Arten konfiguriert werden:

1. Configuration Wizard:	Eine Grundfunktionen der SPHINX kann hier ohne versierten Netzwerkkenntnisse erstellt werden um einen einfachen Einstieg zu gewähren.
2. Learning Mode:	Bei einem Verbindungsaufbau wird ein interaktives Fenster eingeblendet. Sie können sich dann individuell entscheiden.
3. Internet Control Wizard:	Alle Internet-Dienste sind übersichtlich unter-einander aufgelistet.
4. Manuelle Eingabe:	Die Verbindungen können direkt in die White/Black List eingetragen werden.

An einem Beispiel soll hier veranschaulicht werden, wie Sie schnell und einfach eine Konfiguration der Internet-Dienste erstellen können.

Beispiel a:
Sie wollen den Angestellten Ihrer Firma folgende Internet-Dienste erlauben, alle anderen Dienste sollen gesperrt werden:

- Zugriff nur auf die Internetseite Ihrer Firma
- Zugriff auf Ihren Datei- und Druckerserver und andere Server im Netzwerk
- Versenden und Empfangen von E-Mails über Ihren E-Mailserver
- Die Namensauflösung von den Rechnernamen zu IP-Adressen läuft über einen DNS-Server

Lösung:

So erstellen Sie die Grundkonfiguration:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Wizard"
4. Gehen Sie alle Schritte des "Configuration Wizard" durch:

Step 1 of 8:	Do you use this computer to view websites? -> Yes
Step 2 of 8:	Do you use this computer to send and receive e-mails? -> Yes
Step 3 of 8:	Do you use this computer to download files and data from the Internet? -> No
Step 4 of 8:	Do you use this computer to subscribe to Newsgroups on the Internet? -> No
Step 5 of 8:	Do you use this computer to chat online on the Internet via IRC and ICQ? -> No
Step 6 of 8:	Do you use this computer to share files or print from a network? -> Yes
Step 7 of 8:	Do you wish to have the ability to access the Internet at all times? -> Yes

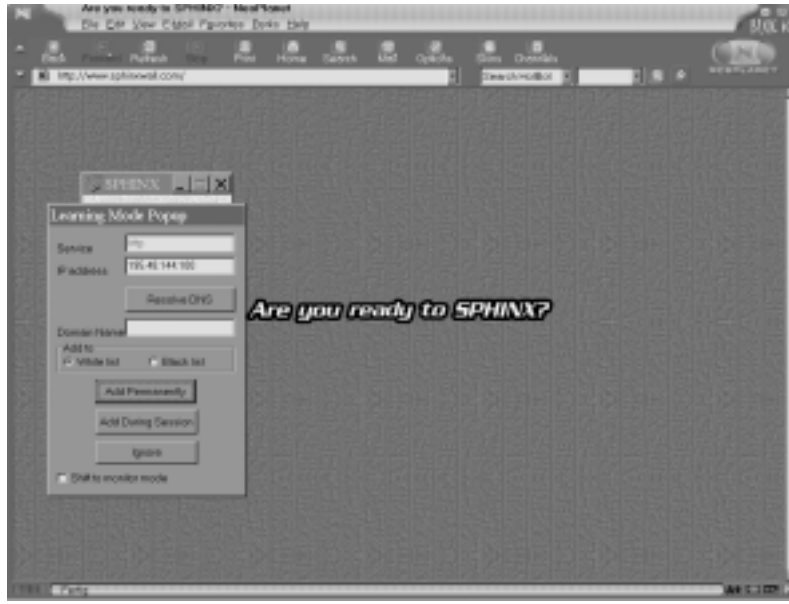
5. Im Schritt 8 von 8 erhalten Sie dann folgende Übersicht:

Zugriff nur auf die Internetseite Ihrer Firma:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Internet control"
4. Wählen Sie den Dienst "Web" aus
5. Klicken Sie auf "Ask for Action":

6. Achten Sie darauf, dass im Logging / Warning-Fenster die Option "Enable all warnings", "Interactive Mode" und "Learning mode ON" angewählt ist:

7. Klicken Sie "Apply" um die Konfiguration zu aktivieren
8. Öffnen Sie nun einen beliebigen Webbrowser und geben Sie die URL Ihrer Internetseite ein
9. Nach einer Weile erscheint ein Fenster (Learning mode popup):



10. Sie können sich entscheiden, ob der Zugriff auf diese Internetseite erlaubt (White list) oder verboten (Black list) ist. Klicken Sie hier bitte auf "White list".
11. Die entsprechenden Filterregeln werden, je nach Auswahl,
    a. permanent (Add permanently),
    b. nur für diese Session (Add during session)
    c. oder gar nicht (Ignore)

    berücksichtigt und entsprechend eingetragen. Klicken Sie hier bitte auf "Add permanently"

12. Überprüfen Sie bitte den Eintrag unter „Internet control":

12. Bei Querverweisen Ihrer Internetseite wählen Sie diese an und gehen, wie in den Schritten 9 bis 11 beschrieben, vor.
13. Nun stellen Sie bitte den Dienst "Web" auf "White list". Alle Eintragungen in der "White list" werden nun von der SPHINX berücksichtigt
14. Im Logging / Warning-Fenster die Option "Enable all warnings" und "Learning mode" auf OFF stellen und dann den "Monitor mode" auswählen:

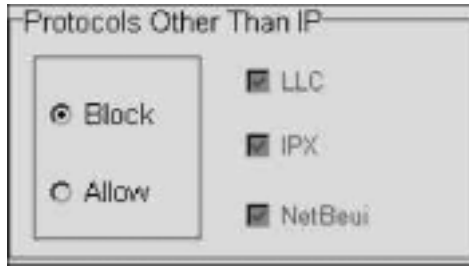
15.Klicken Sie "Apply" um die Konfiguration zu aktivieren.

7. Warum NetBEUI-, IPX- und LLC-Protokolle sperren?

Für die Kommunikation von Rechnern in einem Netzwerk sollte möglichst nur ein Transportprotokoll verwendet werden. Heute hat sich IP als Standardprotokoll durchgesetzt. Um eventuelle Sicherheitsrisiken auszuschalten die durch andere Protokolle entstehen können, sollten diese auf Ihrem Rechner gesperrt werden.

So sperren/erlauben Sie NetBEUI-, IPX- und LLC-Protokolle:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Wählen Sie unter der Option "Protocols other Than IP" ob Sie andere Protokolle außer IP sperren ("Block") oder bestimmte erlauben ("Allow") wollen. Es ist sinnvoll, alle nichtbenötigten Protokolle zu sperren.
5. Wenn Sie "Allow" ausgewählt haben, können Sie die folgenden Protokolle erlauben (einfach das entsprechende Protokoll anklicken):
   a. LLC
   b. IPX
   c. NetBEUI
6. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.



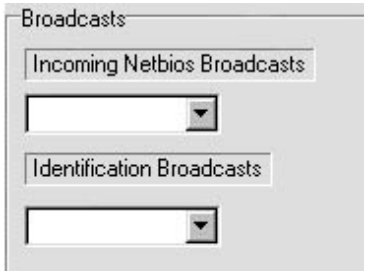
7.1 Warum die NetBIOS Broadcasts sperren?

Sehr populäre Angriffsmethoden sind die sogenannten »Nukes«. Hierzu werden spezielle Datenpakete, die ein besonderes Merkmal haben, an einen Rechner geschickt. Entsprechend ungesicherte Betriebssysteme quittieren den Empfang solcher Pakete mit dem völligen Systemstillstand.

Die speziellen Datenpakete (Out of Band-Packets) bestehen aus manipulierten UDP-Paketen, welche gewöhnlich an den NetBIOS-Port gesendet werden, da dieser bei vielen Computern standardmäßig geöffnet ist. Prinzipiell funktioniert es aber auch mit allen anderen Ports, die für den Datenempfang standardmäßig geöffnet sind. Die Wirkungsweise liegt nun darin, dass ein entsprechend ungesichertes Betriebssystem mit "Out of Band"-Informationen nichts anfangen kann, und im ungünstigsten Fall den Rechner mit einem Systemabsturz lahm legt.

So sperren Sie NetBIOS Broadcasts:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Unter der Option "NetBIOS" stellen Sie folgende Konfiguration ein:
   a. "Incoming NetBIOS Broadcasts" auf "Drop" oder "Advanced"
   b. "Identification Broadcasts" auf "Block" oder "Advanced"
5. Haben Sie "Advanced" eingestellt, klicken Sie das Fenster "Advanced" an
6. Hier haben Sie nun die Möglichkeit, spezielle Filterregeln festzulegen
7. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.



7.2 Warum ICMP sperren?

Das "Ping Flooding" gehört zu den Angriffen, die eigentlich keine Sicherheitslöcher ausnutzen. Pings werden benutzt, um die Erreichbarkeit von anderen Hosts im Netz zu prüfen. Ein »angepingter« Host quittiert einen Ping mit einer Antwort, einem sogenannten »echo replay«. Hierbei wird das ICMP-Protokoll benutzt.

Beim Ping Flooding wird ein Host nun mit unzähligen Ping-Anfragen bombardiert, die der Host alle bearbeitet (falls keine entsprechenden Mechanismen die Abarbeitung von rasch wiederholenden Ping-Anfragen verhindert) und entsprechend das eigene System und die Netzverbindung auslastet.
Ping Flooding ist einer der Angriffe, die sehr teuer werden können: Wird eine Netzverbindung eines Hostes nämlich nach dem erzeugten Datenaufkommen abgerechnet, können teilweise horrende Summen entstehen.

So sperren Sie ICMP:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Unter der Option "ICMP" stellen Sie entweder "Drop" oder "Advanced" ein
5. Haben Sie "Advanced" eingestellt klicken Sie das Fenster "Advanced" an
6. Hier haben Sie nun die Möglichkeit, spezielle Filterregeln festzulegen
7. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.

8. Was sind IP Fragmente und welche Gefahren ergeben sich daraus?

Wenn ein Datenpaket auf seinem Weg zum Zielrechner durch verschiedene Netze geroutet wird, kann der Fall eintreten, daß die MTU (Maximal Transmission Unit) der Netze unterschiedlich sind. Wenn das IP-Paket größer als die MTU des Netzes ist, muß IP das Paket in kleinere Fragmente aufteilen. Dieser Vorgang wird Fragmentierung genannt. Diese Fragmente werden dann im Zielrechner wieder zusammengefügt Dies bezeichnet man als Defragmentierung.

Es gibt nun unterschiedliche Formen, um die IP Fragmente für eine Attacke zu nutzen:

Tiny-Fragment-Attack

Ziel dieser Attacke ist es, durch geschickte Fragmentierung von IP-Pakten, Filterregeln eines Paketfilters zu umgehen. Dabei versucht der Angreifer, seine Nutzdaten (z.B. TCP-Pakete) in so kleine Fragmente zu zerlegen, dass ein statischer Paketfilter seine Regeln bezüglich des TCP-Headers nicht mehr anwenden kann. Paketfilter, die nur das erste Fragment untersuchen, könnten Beispielsweise dadurch ausgetrickst werden, indem man im ersten Fragment nur einen Teil des TCP-Headers ablegt, z.B. nur den Source Port, Destination Port und die Sequence Number. Im zweiten Fragment werden die restlichen TCP-Header Informationen (ACK-Bit, Flags usw.) abgelegt. Kann das erste Fragment den Filter passieren, so könnte ein Angreifer eine eingehende TCP-Verbindung z.B. TELNET durch den Filter schleusen.

Overlapping-Fragment-Attack

Dieser Angriff ist auch unter dem Namen „Teardrop" bekannt. Die zweite Variante macht sich eine Eigenart des derzeitigen Reassemblierungsalgorithmus von IP zunutze. Der Algorithmus lässt es zu, dass neu eingetroffene Fragmente Teile von bereits empfangenen Fragmenten überschreiben können. Dadurch ist es einem Angreifer möglich, eine Folge von Paketen zu erzeugen, in denen das erste Fragment harmlose TCP-Header-Informationen enthält, die ein Paketfilter durchläßt.
Ein zweites Fragment mit einem Offset größer als Null könnte nun andere TCP-Header-Informationen enthalten. Wird der Offset des zweiten Fragments nun kleiner gewählt als die Größe des ersten Fragmentes, so können die TCP-Header-Informationen des ersten Fragmentes durch die des zweiten überschrieben werden.

Ping of Death

Besonders hinterhältige Angriffe sind die »Large Packet-Attacks«, unter Insidern »Ping of Death« genannt (obwohl die Attacke nichts mit dem eigentlichen Ping-Programm zu tun hat).

Die Wirkungsweise von Large Packet-Attacks ist zugleich einfach und fatal: Das IP-Protokoll verpackt alle Daten beim Absender in 64 KB große Päckchen. Diese werden jedoch protokollintern vor der Übertragung in kleinere Päckchen zerlegt, um sie einfacher übertragen zu können (fragmentieren). Beim Empfängerrechner werden diese einzelnen Päckchen wieder zusammengefügt (reassemblieren), allerdings erst, wenn alle Einzelteile vorliegen. Ist das ankommende Paket am Ende größer als 64 KB, läuft ein interner Speicherpuffer über und bringt im ungünstigsten Fall den Rechner zum Absturz.

So sperren Sie IP Fragments:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Unter der Option "IP Fragments" stellen Sie entweder "Drop" oder "Advanced" ein
5. Haben Sie "Advanced" eingestellt klicken Sie das Fenster "Advanced" an
6. Hier haben Sie nun die Möglichkeit, spezielle Filterregeln festzulegen
7. Anmerkung: Die Einstellungen im Fenster „General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.

9. Was ist IP Spoofing?

IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Nummern verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen. Ein Hacker hört mit seinem Rechner C den Datenverkehr von zwei Rechnern A und B mit. Dabei muss er die Parameter der Verbindung aufzeichnen, um sie später nachbilden zu können. Will er in Rechner A einbrechen, so muss er zuerst Rechner B außer Gefecht setzen. Dies kann z.B. durch das fortgesetzte Senden von Verbindungsanforderungen, die nie quittiert werden, geschehen. Jetzt hat er freie Bahn, um beim Rechner A als Rechner B einzubrechen. Dabei muß er sich exakt wie Rechner B verhalten, was durch das Vortäuschen seiner IP-Adresse und anderer Protokollparameter leicht realisierbar ist. In größeren Netzwerkumgebungen reicht es meist, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

Die SPHINX greift in die untersten Netzwerkschichten (OSI-Referenzmodell) ein und gibt einem Angreifer daher keine Möglichkeit, Parameter der Netzwerkverbindung, wie z.B. die IP-Adresse, zu ändern. Wird die IP-Adresse des PC's geändert, werden die IP-Packete mit dem geänderten Absender von der SPHINX verworfen. Die eigentliche IP-Nummer wird fest in der SPHINX eingestellt.

So aktivieren Sie "IP Spoofing protect":

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Klicken Sie auf "IP Spoofing protect" bis das Häkchen erscheint
5. Die IP-Adresse wird bei der Installation der SPHINX automatisch eingetragen, kann aber auch auf einen beliebigen Wert gesetzt werden. Wenn Sie sich nicht sicher sind welche Adresse hier eingetragen werden muss, übernehmen Sie einfach die Standardeinstellungen
6. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.

10. Warum ARP/RARP sperren?

In einer Netzwerkumgebung wird die Kontaktaufnahme untereinander über ARP realisiert. Will man sicherstellen, dass z.B. zwei Rechner ausschließlich miteinander kommunizieren können, deaktiviert man das ARP. Es muss allerdings beiden Rechnern die physikalische und logische Adresse des jeweils anderen Rechner bekannt sein. In größeren Netzwerkumgebungen ist es meist nicht sinnvoll das ARP zu sperren. Bei Verbindungen per Modem dagegen erfüllt das ARP keine Aufgabe und kann bedenkenlos deaktiviert werden. Im Gegensatz zum ARP gibt es für RARP nur wenige Anwendungsfälle. Deshalb kann RARP ebenfalls sowohl in der Netzwerkumgebung als auch bei Modemverbindungen deaktiviert werden.

So sperren Sie ARP/RARP:

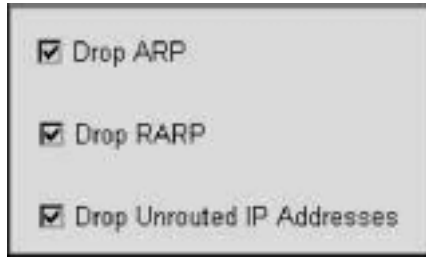
1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Klicken Sie auf "Drop ARP" bis das Häkchen erscheint
5. Klicken Sie auf "Drop RARP" bis das Häkchen erscheint
6. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.

11. Was sind „unroutet IP addresses"?

Im Internet werden nur bestimmte IP-Adressbereiche geroutet, die sogenannten offiziellen IP-Adressen. Manche Angriffe basieren nun auf Adressen, die im Internet nicht weitergeleitet werden. Der Angreifer besitzt zwar eine offizielle Adresse, verschleiert aber seine Identität, indem er seine abgehenden Datenpakete manipuliert. Er baut in diese Pakete einfach als Absenderadresse eine Adresse aus einem inoffiziellen Bereich (unroutet IP addresses) ein. Viele lokale Netzwerkumgebungen benutzen allerdings diesen Adressbereich.

So sperren Sie inoffizielle Adressen:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf "Advanced" und gehen dann auf "Configuration"
3. Klicken Sie auf "Policy"
4. Klicken Sie auf "Drop unroutet IP addresses" bis das Häkchen erscheint
5. Anmerkung: Die Einstellungen im Fenster "General Policy" können Sie auch mit dem "Policy Wizard" schnell und bequem vornehmen.



12. Wie kann ich mich vor einem trojanischem Pferd schützen?

TROJANISCHE PFERDE, kurz TROJANER oder HINTERTÜREN sind Programme, welche meist versteckt in anderen Programmen oder Bildern den Rechner eines Opfers außer Betrieb setzen. Sie können sogar Unberechtigten den Zugang zu dem Rechner verschaffen. Trojanische Pferde vermehren sich im Gegensatz zu Viren nicht selbstständig und sind gerade aus diesem Grund schwer aufzuspüren!

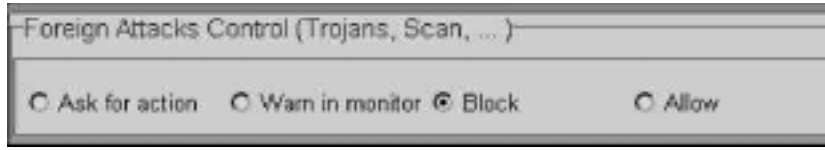
Immer wieder wird in den Medien davor gewarnt, Programme aus unbekannten Quellen auf seinem Computer auszuführen. Dazu gehören z.B. Programme von Internet-Seiten, die einem nicht bekannt sind oder auch von vorneherein etwas merkwürdig erscheinen. Aber auch E-mails die einen Dateianhang besitzen, sind mit Vorsicht zu genießen, selbst wenn diese von einer bekannten Absenderadresse verschickt wurden.

Zu den bekanntesten Programmen der Trojaner zählen z.B. Back Orifice, NetBus oder SubSeven. Sie wurden eigentlich zur Fernwartung von Systemen entwickelt. Diese Programme werden jedoch dazu missbraucht, heimlich auf einem Opfersystem installiert zu werden, um dieses dann auszuspionieren. Die gewonnenen Informationen werden an den Angreifer übermittelt, z.B. per E-Mail, FTP, ICQ, IRC, NNTP (Newsgroups) oder die Programme „lauschen" an einem bestimmten IP-Port (teils TCP-, teils UDP-Ports) und warten auf eine Verbindung von außen.

Die SPHINX gibt die Möglichkeit sich effektiv gegen solche trojanischen Pferde zu schützen. Man kann individuell festlegen, was geschehen soll, wenn von außen versucht wird, eine Verbindung zu Ihrem Rechner herzustellen. Ebenso ist es möglich, ein Zeitlimit für bestehende Verbindungen nach außen einzustellen. Dienste, wie z.B. E-Mail, FTP, usw., die nicht benötigt werden, können durch die SPHINX gezielt blockiert werden.

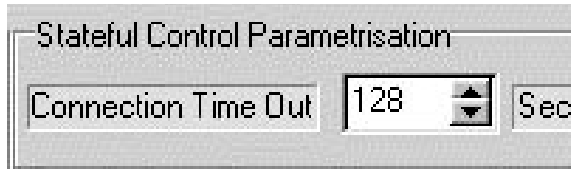
So kontrollieren Sie allgemein Verbindungen von außen:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf „Advanced" und gehen dann auf „Configuration"
3. Klicken Sie auf „Policy"
4. Unter der Option „Foreign attacks control" haben Sie mehrere Einstellungsmöglichkeiten:
5. „Ask for action", hierbei wird bei jedem Versuch, mit Ihrem Rechner eine Verbindung herzustellen, ein interaktives Auswahlfenster eingeblendet
6. „Warn in monitor", hierbei wird bei jedem Versuch, mit Ihrem Rechner eine Verbindung herzustellen, ein Eintrag in den „Warning monitor" geschrieben
7. „Block", alle Verbindungen von außen auf Ihren Rechner werden unterbunden
8. „Allow", alle Verbindungen von außen auf Ihren Rechner sind ausdrücklich erlaubt
9. Anmerkung: Die Einstellungen im Fenster „General Policy" können Sie auch mit dem „Policy wizard" schnell und bequem vornehmen.



So kontrollieren Sie Ihre Verbindungen nach außen:

I. Zeitlimit setzen:
   1. Öffnen Sie die SPHINX Personal Firewall
   2. Klicken Sie auf „Advanced" und gehen dann auf „Configuration"
   3. Klicken Sie auf „Policy"
   4. Unter der Option „Stateful control parametrisation" können Sie nun ein Zeitlimit für Verbindungen nach außen setzen. Antwortet die Gegenstelle, mit der sie verbunden sind, nicht innerhalb der angegebenen Zeit, wird die Verbindung von der SPHINX abgebrochen. Grundbedingung dazu ist dass die ausgehende Verbindung generell erlaubt ist.
   5. Anmerkung: Die Einstellungen im Fenster „General Policy" können Sie auch mit dem „Policy wizard" schnell und bequem vornehmen.



II. Einzelne Dienste sperren/erlauben:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf „Advanced" und gehen dann auf „Configuration"
3. Klicken Sie auf „Internet control"
4. Wählen Sie nun den entsprechenden Dienst aus, z.B. DNS
5. Stellen Sie unter der Option „Action" ein ob Sie den Dienst sperren („Block all") oder erlauben („Allow all") wollen. Es ist sinnvoll alle nichtbenötigten Dienste zu sperren.
6. Anmerkung: Die Einstellungen im Fenster „Internet control" können Sie auch mit dem „Internet control wizard" schnell und bequem vornehmen.

13. Warum bekommen manche Client-Server Anwendungen keine Verbindung mehr?

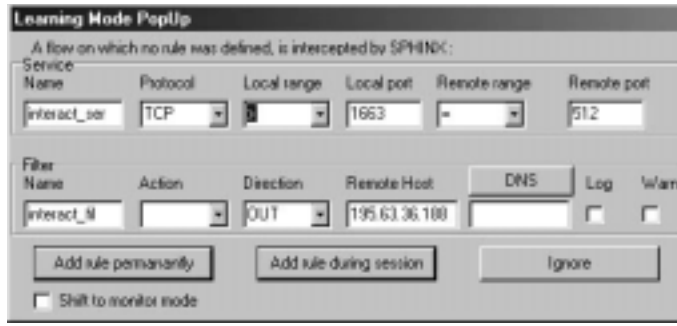
Die meisten Client-Server Anwendungen benutzen zur Kommunikation das TCP- oder UDP-Protokoll. Um eine eindeutige Zuordnung zu der jeweiligen Anwendung zu bekommen, verwenden diese Protokolle sogenannte Ports. Man unterscheidet „well- known ports", die bereits seit langem definiert sind und weltweit Verwendung finden. Sie umfassen einen Bereich von 0 bis 1023. Alle übrigen Ports im Bereich von 1024 bis 65535 stehen den Programmierern für ihre eigenen Entwicklungen zur Verfügung. Manche Client-Server Anwendungen benutzen jedoch Ports aus dem Bereich von 0 bis 1023. Da es sich dabei um nicht festgeschriebene Dienste handelt müssen diese in der SPHINX explizit freigegeben werden.

So geben sie spezielle Ports frei:

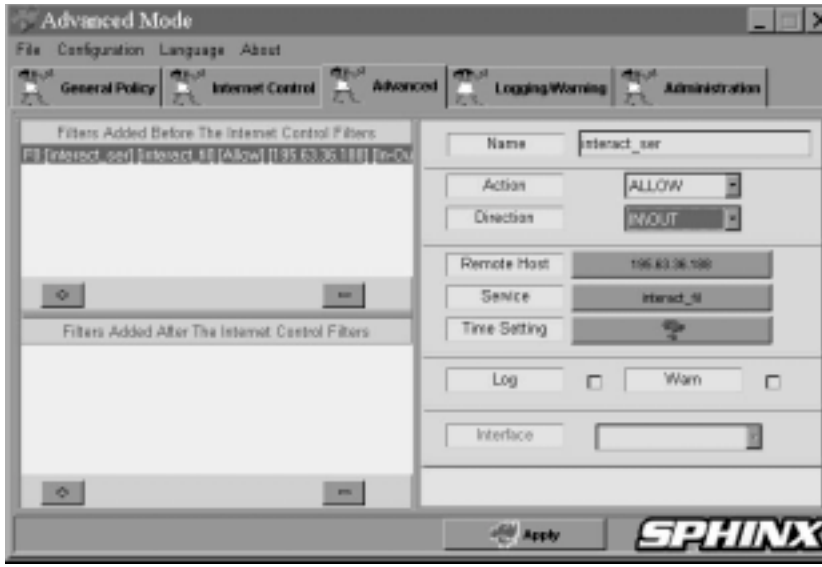
Mit Hilfe der SPHINX können Sie schnell und einfach TCP / UDP-Ports freigeben:

1. Öffnen Sie die SPHINX Personal Firewall
2. Klicken Sie auf „Advanced" und gehen dann auf „Configuration"
3. Klicken Sie auf „Logging / Warning"
4. Aktivieren Sie die Option „Enable all warnings", „Interactive Mode" und „Learning mode ON":

5. Öffnen Sie nun Ihre Client-Server Anwendung
6. Nach einer Weile erscheint ein Fenster (Learning mode popup):



7. In diesem Fenster werden die genauen Daten der Verbindung angezeigt:
   a. das verwendete Protokoll
   b. der lokale Port (Quell-Port)
   c. der Port des Servers (Ziel-Port)
   d. die IP-Adresse des Servers
8. Die entsprechenden Filterregeln werden, je nach Auswahl,
   a. permanent (Add permanently),
   b. nur für diese Session (Add during session)
   c. oder gar nicht (Ignore)
   berücksichtigt und entsprechend eingetragen
9. Da die Adresse und der verwendete Port des Servers somit eindeutig definiert ist und der lokale Port des eigenen Rechners sich bei jeder Verbindung immer wieder ändert (zwischen 1023 und 65535), sollte der lokale Port auf „>1022" gesetzt werden
10. Damit die Verbindung sowohl nach innen als auch nach außen aufgebaut werden kann, sollte als Richtung „in/out" gewählt werden
11. Überprüfen Sie bitte den Eintrag unter „advanced":



12. Klicken Sie „Apply" um die Konfiguration zu aktivieren