Michael Calmer, Uwe Gansert, Dennis Geider, Viviane Glanz, Roland Haidl,
Edith Parzefall, Peter Reinhart, Ulrich Schairer, Thomas Schraitle,
Martin Sommer, Marius Tomaschewski, Rebecca Walter

SuSE Linux Firewall on CD — VPN Edition

SuSE GmbH
Schanzäckerstr. 10
D-90443 Nürnberg
Tel.: (0911) 740 53 0
Fax: +49-911-740-479
E-Mail: suse@suse.de
WWW: http://www.suse.de

Michael Calmer, Uwe Gansert, Dennis Geider, Viviane Glanz, Roland Haidl, Edith Parzefall, Peter Reinhart, Ulrich Schairer, Thomas Schraitle, Martin Sommer, Marius Tomaschewski, Rebecca Walter

SuSE Linux Firewall on CD
—VPN Edition
1. Auflage 2001

Inhaltsverzeichnis

1 Vorwort

Die Autoren bedanken sich bei Jürgen Scheiderer, Carsten Höger, Remo Behn, Thomas Biege, Roman Drahtmüller, Marc Heuse und Stephan Martin.

Die SuSE Linux Firewall on CD

Mit der *SuSE Linux Firewall on CD* haben Sie ein Werkzeug an der Hand, mit dem Sie eine Firewall-Lösung für Ihr Netzwerk einrichten, überwachen und warten können. Für diese Aufgaben stehen Open-Source-Programme zur Verfügung, die speziell dafür ausgewählt und weiterentwickelt wurden.

Die *SuSE Linux Firewall on CD* schützt Ihr lokales Netzwerk gegen unberechtigte Zugriffe und reglementiert erlaubte Zugriffe auf Ihre Ressourcen. Sie bietet Ihnen auch die Möglichkeit, den Zugang Ihres lokalen Netzwerks in das Internet zu steuern und zu regeln.

Die Wahrscheinlichkeit eines Konfigurationsfehlers im Firewall-Setup verringern Sie durch die Verwendung des *Firewall Administration System*s (FAS). Fehler durch den Anwender werden weitestgehend durch Plausibilitätsprüfungen abgefangen. FAS sorgt für eine konsistente Konfiguration, ohne die Konfigurationsmöglichkeiten einzuschränken.

Allerdings kann keine Firewall absolute Sicherheit bieten. Das gilt auch für die „SuSE Linux Firewall on CD“, die keine Security-Policy ersetzt. Durch sie wird auch die Wartung, Pflege und Überwachung der Firewall nicht überflüssig, aber sie stellt Werkzeuge zur Verfügung, die diese Aufgaben erleichtern.

Hinweis

Die Verwendung des Produkts „SuSE Linux Firewall on CD“ erfolgt auf eigenes Risiko. Insbesondere für Datenverlust durch fehlerhaft konfigurierte Dienste auf der Firewall und für sonstige Schäden besteht kein Anspruch auf Schadenersatz.

1 Vorwort

2 Einführung und Allgemeines

2.1 Einführung

Die Bedeutung des Internets und die damit verbundenen Möglichkeiten der Kommunikation (E-Mail, Chat etc.) und der Informationsbeschaffung wachsen stetig. Immer mehr Unternehmen und Privatpersonen verfügen heute über einen Zugang zum Internet.

Die Anbindung an das Internet ist jedoch häufig mit einigen nicht zu unterschätzenden Risiken verbunden. Die meisten Unternehmen betreiben ein eigenes Netzwerk, in dem unternehmenskritische Informationen für den internen Gebrauch weitergegeben und verarbeitet werden (Intranet, Datenbanken, E-Mails etc.). Ohne geeignete Schutzmaßnahmen sind diese Informationen durch die Anbindung an das Internet für jedermann offen zugänglich. Dadurch kann gerade für Firmen ein nicht unerheblicher Schaden entstehen.

> Es ist einfach, ein Computersystem sicher zu betreiben. Sie müssen bloß alle Wählverbindungen abklemmen, ausschließlich direkt angeschlossene Terminals zulassen, diese Terminals und den Computer selbst in einen abgeschirmten Raum bringen sowie eine Wache vor die Tür stellen.
>
> F.T. Grampp und R.H. Morris

Der Betrieb eines Computersystems in dieser Weise ist natürlich nicht möglich. Sie als Administrator wissen, welche Probleme sich aus der zunehmenden Vernetzung ergeben und sind tagtäglich damit konfrontiert. Bislang war Ihr Netz noch relativ überschaubar und die Benutzer bekannt. Sicherheitsaspekte hatten zwar schon immer einen sehr hohen Stellenwert, aber die Funktionalität, die das Netz den Benutzern zur Verfügung stellte, basierte in erster Linie auf Vertrauensbeziehungen. Anders wäre ein solches internes Netz nicht mit angemessenem Aufwand zu administrieren. Durch den Internet-Anschluss verändern sich die Rahmenbedingungen für Ihre Administrationstätigkeit zum Teil dramatisch. Plötzlich gibt es Benutzer, die unbekannt sind und Ressourcen Ihres Netzes (z. B. den WWW-Server) nutzen können.

Ihnen ist klar, dass diese Benutzer grundsätzlich anders behandelt werden müssen, als die bisherigen internen Benutzer (auch wenn nachweisbar 80 % der Angriffe auf ein Firmennetz nicht von außen erfolgen). Ein weiterer Grund, den Zugang zum Firmennetz zu begrenzen und zu schützen, ist die Tatsache, dass Cracker oder Hacker immer wieder auf der Suche nach Speicherplatz sind, auf dem sie gehackte/gecrackte Software, oder schlimmer noch, strafrechtlich relevante Inhalte ablegen können. Unter Umständen macht sich die Firma selbst

strafbar, wenn sie keine geeigneten Gegenmaßnahmen ergreift. Es geht also auch um Ihren guten Ruf.

Um unerlaubten Zugriff auf das Firmennetz und dessen Ressourcen (Plattenplatz, CPU-Leistung etc.) zu verhindern, stehen heute verschiedene Schutzmaßnahmen zur Verfügung: Angefangen beim IP-Paketfilter auf einem Router bis hin zur mehrstufigen Firewall-Lösung mit demilitarisierter Zone (DMZ).

Im wörtlichen Sinn ist eine Firewall eine Schutzvorrichtung, die das Ausbreiten eines Feuers verhindern soll. Gebäude haben solche Brandschutzmauern aus Ziegelsteinen, die ganze Gebäudeabschnitte komplett abschotten. In Automobilen trennt ein Abschlussblech den Motorraum von der Fahrzeugkabine. Der Zweck von Internet-Firewalls ist es, Angriffe aus dem Internet von Ihrem Intranet fern zu halten bzw. die Clients in Ihrem LAN durch Zugangsverbot zu reglementieren und zu schützen.

Die erste Computer-Firewall war ein nicht routender Unix Host, der eine Verbindung zu zwei verschiedenen Netzwerken hatte. Das eine Netzwerkinterface war mit dem Internet verbunden, das andere mit einem privaten LAN. Um vom privaten Netzwerk aus in das Internet zu gelangen, musste man sich auf dem Unix Firewall-Server anmelden, um von dort aus Zugang zum Internet zu erhalten. Sie konnten z. B. X-Window benutzen, um einen Browser auf dem Firewall-Rechner zu starten und das Display auf Ihre Workstation legen. Mit dem Browser auf der Firewall hatten Sie Zugriff auf beide Netzwerke. Diese Art von „Dual Homed Systems“ ist nur dann geeignet, wenn Sie allen Ihren Benutzern vertrauen können. Dazu vielleicht ein wichtiger Hinweis: 99 % aller Einbrüche in Computer-Systeme beginnen mit dem Versuch, sich einen Benutzeraccount auf dem angegriffenen System anzulegen.

Entscheidend für den Umfang der Maßnahmen ist der Schutzbedarf, der teilweise durch Gesetze geregelt ist, aber auch durch Kommunikationsanalysen ermittelt werden muss.

Wichtig für den Betrieb einer Firewall ist auch die Dokumentation. Es muss festgehalten werden: „Wer hat wann was wie konfiguriert“, um nachvollziehen zu können, ob Änderungen nur von autorisierter Seite durchgeführt wurden. Dies ist z. B. für Zertifizierungen und Audits wichtig.

Die „SuSE Linux Firewall on CD“ ist das Produkt, das diesen kompletten Bereich, in allen Stufen, vom Paketfilter bis zur mehrstufigen Firewall, abdecken kann. Weil alle verwendeten Programme Open Source sind, ist auch eine Auditierung der Quellcodes ohne größere Schwierigkeiten möglich.

2.2 SuSE Linux Firewall on CD

Die folgenden zwei Produktteile bilden die „SuSE Linux Firewall on CD“:

1. Die „SuSE Linux Live-CD for Firewall“ und
2. die „SuSE Linux Admin-CD for Firewall“ .

Im Folgenden wird der Einfachheit halber meist nur von der Live-CD bzw. der Admin-CD gesprochen. Die Live-CD bildet die eigentliche Firewall, basierend

auf dem Konzept des Application-Level-Gateways, mit IP-Paketfilterung kombiniert. Die Routing- und Gateway-Funktionalität ist standardmäßig ausgeschaltet, lässt sich aber, falls notwendig, aktivieren. Alle Anfragen werden auf Anwendungsebene angenommen und verarbeitet. Unterstützt werden die wichtigsten Internetprotokolle: SMTP, FTP, HTTP, HTTPS, DNS sowie VPN.

Mit der Admin-CD installieren Sie den SuSE Linux Adminhost, der für die Konfiguration, Überwachung und die Wartung der SuSE Linux Firewall vorgesehen ist. Um diesen Aufgaben gerecht zu werden, ist eine spezielle Auswahl an Softwarepaketen im Liefer- und Installationsumfang vorhanden.

Wichtig für die Anbindung eines internen Firmen-Netzes an das Internet ist eine vernünftige Planung und dazu gehört auch die Erstellung eines Sicherheitskonzepts. Dieses umfasst eine Kommunikations- und Bedarfsanalyse, außerdem sollte ein Konzept für den Notfall (Einbruch, Datenverlust usw.) erstellt werden. Sorgen Sie auch dafür, dass niemand unberechtigterweise physikalischen Zugriff auf den Firewall-Rechner hat. Stellen Sie ihn also am besten in einen abgeschlossenen Serverraum.

2.2.1 Netzwerk Planung

Vor dem Einrichten der Firewall sollten Sie sich überlegen, wie Sie das Netzwerk gestalten wollen. Die Diagramme im folgenden Abschnitt stellen verschiedene Möglichkeiten dar. Als erstes sollten Sie allerdings die geeignete Hardware bedenken.

Der eigentliche Firewall-Rechner, auf dem die SuSE Linux Firewall on CD laufen wird, kann nicht zusätzlich für andere Zwecke genutzt werden. Er braucht auf alle Fälle ein Diskettenlaufwerk für die Konfigurationsdiskette und ein bootfähiges CD-ROM-Laufwerk, sowie eine Festplatte, falls Sie Squid oder Postfix verwenden wollen.

Der Adminhost sollte ebenfalls ein Rechner sein, der ausschließlich dem Zweck dient, die Konfiguration der Firewall zu erstellen und auf Diskette zu speichern. Das Firewall Administration System (FAS), mit dem die Konfiguration erstellt wird, läuft auf einer graphischen Benutzeroberfläche. Alle Programme, die Sie dazu benötigen, befinden sich auf der Admin-CD. Der Adminhost kann darüberhinaus als Log-Rechner benutzt werden, wenn Sie dafür keinen zusätzlichen Rechner verwenden wollen.

Der Log-Rechner zeichnet alle Vorgänge auf dem Firewall-Rechner auf, deshalb benötigt er eine Festplatte mit großer Kapazität. Die Verbindung zwischen Log-Rechner und Firewall-Rechner sollte niemals unterbrochen werden.

2.2.2 Übliche Firewall-Setups – Übersicht

Im Folgenden stellen wir Ihnen ein paar übliche Setups für Firewall-Systeme vor. Alle hier dargestellten Lösungen sind mit der „SuSE Linux Firewall on CD“ realisierbar.

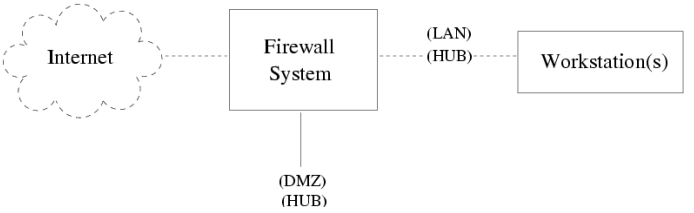


Abbildung 2.1: Einfachstes Setup

Abbildung 2.1 zeigt einen Firewall-Rechner mit drei Netzwerkinterfaces: Extern zum Internet, Intern über LAN/HUB ins Firmennetz und über einen HUB zur DMZ (demilitarisierte Zone).

Die Firewall muss also Defaultgateway (Router), Paketfilter usw. sein. Sie ist der einzige Schutz. Wenn sie überwunden wird, ist das interne Netz nicht mehr gegen Angriffe geschützt.

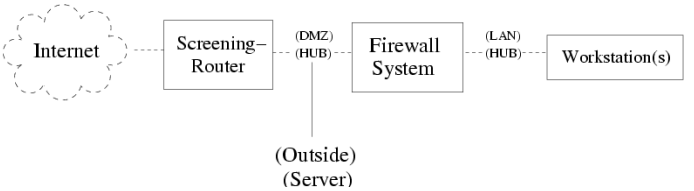


Abbildung 2.2: Einfaches Setup

Abbildung 2.2 zeigt ein immer noch relativ einfaches Setup. Die DMZ ist nur durch einen Paketfilter auf dem Router (Screening Router) geschützt.

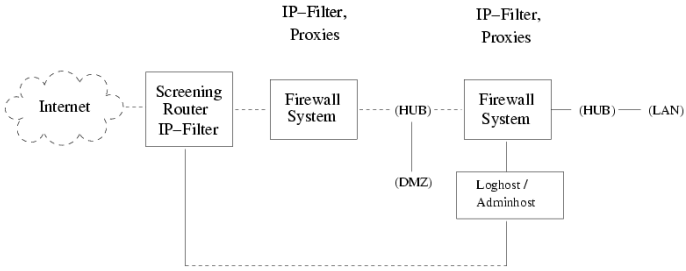


Abbildung 2.3: Überschaubares und effektives Setup

Abbildung 2.3 zeigt eine immer noch überschaubare, aber dennoch wesentlich effektivere Lösung.

Ein „Screening Router“ blockt auf Paketebene unberechtigte Zugriffe ab. Nachgeschaltet ist ein erster Firewallrechner, der auf Applikationsebene und durch Paketfilter-Regeln den Zugriff auf die DMZ sowie den zweiten Firewall-Rechner und damit auf das interne Netz regelt. Der zweite Firewall-Rechner schützt das interne Netz auf Paketfilter- und Proxy-Basis und regelt darüber hinaus die Zugriffe aus dem internen Netz auf das Internet und die DMZ. Der Admin-Rechner ist in einem gesonderten Netz, das mit den Firewall-Systemen verbunden ist.

3 SuSE Linux Adminhost for Firewall

Eine Firewall zu administrieren, zu warten und zu überwachen ist keine leichte Aufgabe, vor allem darf deren Überwachung nicht auf die leichte Schulter genommen werden. Deshalb befindet sich im Lieferumfang der „SuSE Linux Firewall on CD“ der „SuSE Linux Adminhost for Firewall“, der es Ihnen erleichtern soll, die SuSE Linux Firewall zu konfigurieren, zu administrieren und zu pflegen.

3.1 Einführung

Nach der Installation des SuSE Linux Adminhost for Firewall steht Ihnen mit dem Firewall Administration System (FAS) ein Werkzeug mit graphischer Administrationsoberfläche zur Verfügung, das es Ihnen ermöglicht, menügeführt die Konfiguration der „SuSE Linux Live-CD for Firewall“ vorzunehmen.

Für die Überwachung der Firewall stehen konfigurierbare Werkzeuge zur Verfügung, mit denen Tests der Firewall, Auswertung der Log-Dateien und Überwachung des Netzwerkverkehrs durchgeführt werden können. Im Falle eines Angriffs besteht die Möglichkeit, die Systemadministration per E-Mail, Pager usw. zu benachrichtigen, damit möglichst frühzeitig geeignete Gegenmaßnahmen ergriffen werden können (z. B. Trennen der Netzverbindung zum Internet/Intranet etc.).

Hier zeigt sich auch schon, dass eine Firewall ohne laufende Überwachung keinen echten Schutz bieten kann. Außerdem sollten alle Änderungen, die an der Konfiguration der Firewall vorgenommen wurden, durchgehend und vollständig dokumentiert werden. Anhand der Dokumentation können Fehler leichter gefunden werden oder auch Änderungen, die von unautorisierter Seite kommen, wieder zurückgenommen werden.

Bei der Installation des „SuSE Linux Adminhost for Firewall“ haben Sie die Wahl zwischen einer Neuinstallation des dafür vorgesehenen Rechners und einem Update, falls auf diesem Rechner bereits SuSE Linux 7.2 oder der SuSE Linux Enterprise Server 7 installiert ist. Im folgenden Abschnitt beschreiben wir das Update, anschließend die Neuinstallation des „SuSE Linux Adminhost for Firewall“

3.2 Update

Wenn Sie auf dem Rechner, der als Adminhost für die Firewall dienen soll, bereits SuSE Linux 7.2 oder der SuSE Linux Enterprise Server 7 installiert haben,

müssen Sie keine Neuinstallation durchführen, sondern können auch nur die notwendigen Pakete nachinstallieren. Sie können dabei zwischen dem graphischen Installationsprogramm YaST2 oder dem textbasierten YaST wählen.

Hinweis

Falls Sie bereits die SuSE Linux Firewall on CD betreiben und nun auf die VPN Edition updaten möchten, müssen Sie nur die fas-Pakete mit YaST oder YaST2 durch die im folgenden Abschnitt aufgeführten fas2-Pakete ersetzen.

Leider sind die Konfigurationen, die mit der Vorgängerversion erzeugt wurden, inkompatibel zu den Konfigurationen die FAS2 erstellt. Sie können allerdings diese bestehenden Konfigurationen mit einem Skript konvertieren.

Rufen Sie als `'root'` das Skript mit dem Befehl **`fas_convertconfig.pl`** auf und folgen Sie den Anweisungen des Programms. Das konvertierte tar-Archiv der Konfiguration wird den gleichen Namen erhalten wie das Original und an derselben Stelle liegen.

3.2.1 Update mit YaST2

Um ein Update eines SuSE Linux 7.2 System oder eines SuSE Linux Enterprise Server 7 auf die die Firewall on CD – VPN Edition durchzuführen, gehen Sie wie folgt vor:

1. Melden Sie sich als Benutzer `'root'` an der graphischen Konsole an.
2. Starten Sie das YaST2-Kontrollzentrum und wählen Sie unter YaST2 Module den Menüpunkt '`Software`' aus.
3. Legen Sie die CD mit der Aufschrift *SuSE Linux Adminhost for Firewall* ein.
4. Unter dem Menüpunkt '`Change Source Media`' wählen Sie bei Quellmedium '`Von CD installieren`' aus.
5. Speichern Sie und beenden Sie den Dialog.
6. Wählen Sie den Menü-Punkt '`Software`', aktivieren Sie die Checkbox '`Paketserien anzeigen`'.
7. Wählen Sie die Serie `zfw` aus und selektieren Sie die Pakete:
   - fas2-flc-dns
   - fas2-flc-base
   - fas2
   - fas2-flc-ftp
   - fas2-flc-ntp
   - fas2-flc-mail

- fas2-flc-http
- fas2-flc-rinetd
- fas2-flc-ipchains
- fas2-flc-ipsec
- fas2-doc
- fasd2
- yast2-config-fwcdadmin
- yast2-trans-fwcdadmin

Die Paketabhängigkeiten werden von YaST2 automatisch aufgelöst.

8. Wenn Sie diesen Rechner gleichzeitig als Loghost verwenden wollen, müssen Sie aus der Serie n das syslog-ng installieren.

3.2.2 Update mit YaST1

1. Melden Sie sich als Benutzer ‘root’ auf einer Konsole an.
2. Legen Sie die CD mit der Aufschrift *SuSE Linux Adminhost for Firewall* ein.
3. Starten Sie YaST.
4. Im YaST Menü wählen Sie den Punkt ‘Paketverwaltung’ aus.
5. Wählen Sie ‘Konfiguration ändern/erstellen’ aus.
6. Wechseln Sie in die Serie zfw1
7. Wählen Sie hier alle Pakete außer Paket fas-devel zur Installation aus:
   - fas2-flc-dns
   - fas2-flc-base
   - fas2
   - fas2-flc-ftp
   - fas2-flc-ntp
   - fas2-flc-mail
   - fas2-flc-http
   - fas2-flc-rinetd
   - fas2-flc-ipchains
   - fas2-flc-ipsec
   - fas2-doc
   - fasd2
   - yast2-config-fwcdadmin
   - yast2-trans-fwcdadmin
8. Die Abhängigkeiten der Pakete werden angezeigt, lösen Sie sie durch Drücken von (F10) im Dialog ‘Nicht erfüllte Abhängigkeiten’ auf.

3.2.3 Update abschließen

Nur wenn Sie das Update von einer SuSE Linux 7.2 oder einem Enterprise Server 7 durchgeführt haven — unabhängig davon, ob mit YaST1 oder YaST2 die Pakete installiert wurden, — müssen Sie zusätzlich noch das YaST2-Modul für den SuSE Linux Adminhost for Firewall mit folgendem Befehl aufrufen:

```
root@adminhost: # /sbin/yast2 fwcdadmin
```

Alternativ können Sie unter KDE2 das YaST2-Kontrollzentrum starten und unter ‘`Netzwerk/Basis`’ das Modul „SuSE Firewall Adminhost“ aufrufen (vgl. Abbildung 3.1).

Abbildung 3.1: YaST2 Control Center

Wenn Sie eine vorhandene SuSE Linux Firewall on CD um die VPN Edition erweitert haben, ist dies nicht notwendig. Allerdings müssen die den fasd-Daemon erneut starten. Als Benutzer ‘`root`’ rufen Sie dazu den Befehl **`rcfasd restart`** auf. Denken Sie auch daran, die Konvertierung der alten Konfigurationen durchzuführen wie im Abschnitt 3.2 auf Seite 17 beschrieben.

3.3 Neuinstallation des SuSE Linux Adminhost for Firewall

Zur Neuinstallation des „SuSE Linux Adminhost for Firewall“ legen Sie bitte die CD mit der entsprechenden Beschriftung in das CD-Laufwerk des Rechners ein und führen einen Reboot durch. Falls der Rechner nicht von CD bootet, müssen Sie im BIOS die Bootsequenz entsprechend ändern.

Der Begrüßungsbildschirm von linuxrc erscheint – drücken Sie einfach (↵), danach startet die automatische Hardwareerkennung.

YaST2 führt Sie nun durch die weitere Installation. Es werden alle für die Administration, Konfiguration und Wartung nötigen Programme installiert.

3.3.1 Sprachauswahl

Mit der Sprachauswahl beginnend werden Sie nun erstmals mit Maus oder Tastatur in den Installationsprozess eingreifen. Alle Eingabefelder, Auswahllisten und Buttons („Schaltflächen“ oder „Knöpfe“) können durch Mausklick angewählt werden. Wenn Sie auf die Tastatur ausweichen wollen, gelten folgende Regeln:

- (Tab) lenkt den Fokus auf einen Bereich, ein Eingabe-/Auswahlfeld oder einen Button; mit (⇧ Umschalt) + (Tab) gelangen Sie zu einer anderen Auswahlgruppe. Mit (↑) und (↓) kann je nach aktiviertem Bereich eine Auswahl getroffen oder in einer Liste geblättert werden.
- Mit (↵) wird das angewählte Kommando ausgeführt; in der Regel ist das die Aktion, die auf dem jeweils aktiven Button genannt ist.
- Mit (Leertaste) können Einträge angekreuzt werden.
- Außerdem können die meisten Aktionen durch die Tastenkombination (Alt) + *unterstrichener Buchstabe* ausgelöst werden.

Tipp

Hier und in den folgenden Dialogen wird YaST2 nur Informationen sammeln. Später wird Ihnen YaST2 diese Erkenntnisse gesammelt in einer Übersicht vorlegen; wie in Abschnitt 3.3.7 auf Seite 24 beschrieben haben Sie immer noch die Möglichkeit, mithilfe des ‘Zurück’-Buttons zu den vorherigen Dialogen zurückzugehen, um Angaben zu korrigieren.

Wählen Sie die Sprache aus, die Sie verwenden möchten und klicken Sie auf ‘Weiter’. Die Texte aller folgenden Dialoge erscheinen dann in der gewünschten Sprache.

3.3.2 Auswahl der Maus

Dieser Dialog wird nur eingeblendet, wenn YaST2 die Maus nicht automatisch erkennen konnte. Ein Dialogfenster mit einer langen Liste von Mausbezeichnungen erscheint, aus der Sie den erforderlichen Maustyp auswählen können. Nachdem Sie den richtigen Typ gefunden haben, gehen Sie mit (Tab) auf den Button 'Testen' und drücken Sie (↵). Bewegen Sie nun die Maus. Wenn sich der Mauszeiger kontrolliert bewegen lässt, ist alles in Ordnung und Sie können mit der Maus auf 'Weiter' klicken. Im Falle eines Fehlversuchs gehen Sie wieder mit (Tab) in die Auswahlliste, um die Einstellung zu berichtigen.

Wenn kein Maustyp funktioniert bzw. Sie gar keine Maus verwenden wollen, aktivieren Sie bitte den Eintrag 'Keine Maus'. Dann wird die weitere Installation nur über die Tastatur gesteuert.

3.3.3 Tastatur und Zeitzone

Wählen Sie nun das Tastatur-Layout und die Zeitzone aus.

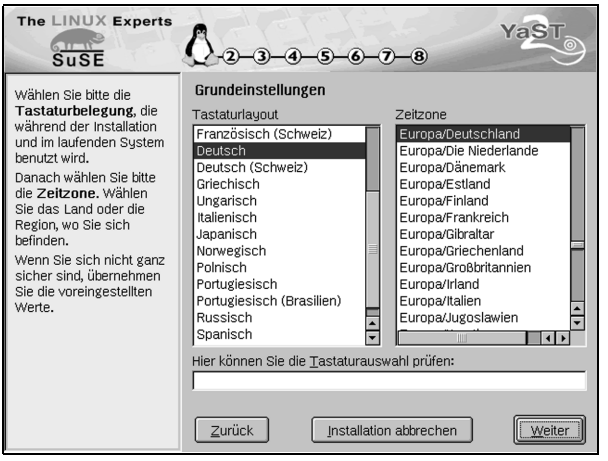


Abbildung 3.2: YaST2: Tastatur und Zeitzone

- Testen Sie bitte Ihre Tastatur. Dazu können Sie mit einem Mausklick oder mit mehrmaligem (Tab) die Eingabezeile aktivieren und dort Buchstaben eingeben. Testen Sie insbesondere 'y'/'z' sowie die Umlaute.

- Als zweiter Punkt steht eine Länderliste zur Verfügung. Wählen Sie Ihr Land bzw. das richtige Teilgebiet aus; YaST2 wird die dazu passende Zeitzone wählen.

Der Button 'Weiter' bringt Sie zum nächsten Dialogfenster.

3.3.4 Festplatte vorbereiten

Bei den folgenden Schritten wählen Sie den Festplattenbereich aus und bereiten diesen auf die Installation von SuSE Linux vor. Je nach Hardware-Konfiguration Ihres Rechners werden die nachfolgenden Dialoge kleinere oder größere Abweichungen von dem hier beschriebenen Beispiel aufweisen.

Schritt 1

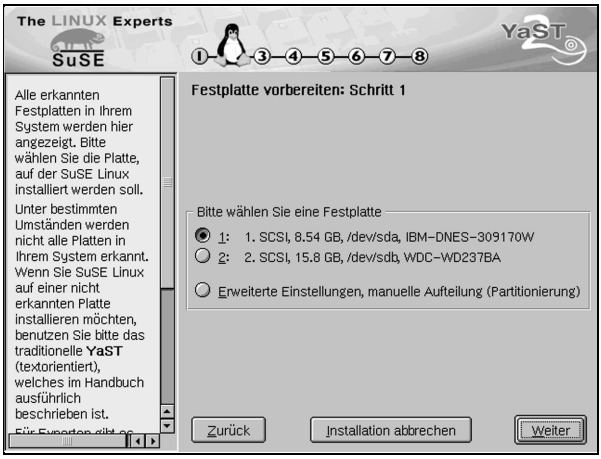


Abbildung 3.3: YaST2: Festplatte vorbereiten (I)

Befindet sich in dem Rechner mehr als eine Festplatte, muss zunächst entschieden werden, welche für die Installation benutzt wird. Die gefundenen Platten werden nacheinander aufgelistet; vgl. Abbildung 3.3.

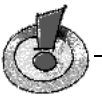
Im Normalfall werden Sie *eine* Festplatte auswählen und danach auf ‘`Weiter`’ klicken.

Schritt 2

Eine der beiden folgenden Situationen kann auftreten:

- Wenn die Festplatte *nicht* leer ist, zeigt YaST2 hier alle bereits auf der Platte befindlichen Partitionen sowie den Punkt ‘`Gesamte Festplatte`’ an. Freier, nicht partitionierter Speicherplatz am Ende der Festplatte wird ebenfalls angezeigt und ist automatisch vorangewählt. Weiteren Platz kann YaST2 nur zusammenhängend nutzen, d. h. Partitionen können nur „von hinten“ her zur zusätzlichen Verwendung freigegeben werden, bei drei eingerichteten Partitionen bleiben beispielsweise Partition 1 und 2 erhalten und Sie kreuzen die dritte zur Freigabe an. Falls Sie sich entscheiden, die gesamte Platte für SuSE Linux zur Verfügung zu stellen, wählen Sie ‘`Gesamte Festplatte`’.
- Eine *leere* Platte wird komplett für SuSE Linux verwendet.

Wenn Sie andere Anforderungen haben, gehen Sie ‘Zurück’ zum letzten Dialog, um dort mit Hilfe der ‘Erweiterten Einstellungen’ manuell zu partitionieren.



Hinweis

Da die angewählten Partitionen, die für SuSE Linux zur Verfügung gestellt werden sollen, formatiert werden, gehen alle dort eventuell vorhandenen Daten unwiederbringlich verloren!

Wenn später die eigentliche Installation beginnt und alle Bedingungen erfüllt sind, wird YaST2 den Plattenplatz selbstständig einrichten. Die gesamte Platte bzw. der freie Platz und/oder die freigegebenen Partitionen werden für SuSE Linux in drei Standard-Partitionen aufgeteilt (und zwar in eine kleine Partition für /boot [etwa 16 MB] möglichst zu Beginn der Platte, eine Partition für Swap [128 MB] und der ganze Rest für /).

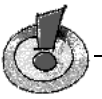
3.3.5 Bootmanager für den Systemstart

Damit Linux später überhaupt starten kann, ist ein Bootmechanismus nötig. Es muss festgelegt werden, an welcher Stelle im System der Bootmanager LILO (engl. *LInux LOader*) installiert wird bzw. ob ein anderes Bootkonzept verwendet werden soll.

3.3.6 ‘root’-Passwort festlegen

Der Benutzer ‘root’ ist unter Linux mit besonderen Privilegien ausgestattet, er kann z. B. Systemprozesse starten/beenden, Benutzer anlegen und entfernen, wichtige Systemdateien manipulieren etc. und übernimmt insofern die Aufgaben eines Systemadministrators.

Sie werden hier dazu aufgefordert, für den Benutzer ‘root’ ein Passwort zu vergeben.



Hinweis

Das ‘root’-Passwort müssen Sie sich unbedingt merken; Sie können es später nicht mehr rekonstruieren. Sie werden das Passwort immer dann brauchen, wenn Sie administrative Aufgaben am System durchführen wollen.

3.3.7 Einstellungen bestätigen – Installation starten

Zur Übersicht und Kontrolle werden alle bisher gesammelten Daten angezeigt. Falls Sie Änderungen vornehmen möchten, gelangen Sie mit ‘Zurück’ schrittweise wieder bis zur ersten Eingabemaske.

Abbildung 3.4: YaST2: Eingabe des ‘root’-Passwortes

Wenn Sie ‘Weiter’ wählen, erfolgt zunächst eine Sicherheitsabfrage (in grün), ob Sie die Installation jetzt tatsächlich mit den angezeigten Einstellungen starten möchten:

- Nach Bestätigung mit ‘Ja - installieren’ beginnt YaST2 mit der Einrichtung des Systems.
- Mit ‘Nein’ haben Sie die Möglichkeit, die Daten erneut zu kontrollieren und gegebenenfalls zu ändern, indem Sie ‘Zurück’ zur entsprechenden Maske gehen.

Sie haben jetzt nochmals die Möglichkeit, die Installation abzubrechen. Alle bisher gemachten Einstellungen und Angaben gehen dann verloren. Wenn Sie ‘Installation abbrechen’ wählen, wird Ihr Rechner nach nochmaliger Rückfrage heruntergefahren und Sie können ihn ausschalten oder neu booten. Auf Ihrem Rechner werden bis zu diesem Zeitpunkt keinerlei Veränderungen vorgenommen.

Über die Funktion ‘Einstellungen auf Diskette speichern’ können Sie alle Angaben auf Diskette speichern, um Sie bei weiteren Installationen wieder abrufen zu können. Dieser Punkt kann nur dann gewählt werden, wenn Ihre Hardware dies zulässt.

In der Regel werden Sie sich für ‘Ja - installieren’ entscheiden. Es werden Partitionen angelegt und formatiert. Je nach Systemausstattung und Größe der Festplatte wird dies einige Zeit in Anspruch nehmen. Vermeiden Sie einen Abbruch, da Sie damit die Festplatte in einen undefinierten Zustand versetzen würden.

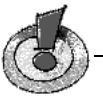
Anschließend werden die Pakete von der CD eingelesen, das SuSE Linux-Basissystem installiert und der Bootmanager eingerichtet. Nach der Bestätigung mit ‘OK’ wird dieses textorientierte Basissystem gestartet. YaST2 setzt die Installation der Software fort; wenn Sie während dieser Phase die Installation abbrechen, wird das System in einem unbenutzbaren Zustand sein!

Es fehlt noch die Vorbereitung der grafischen Oberfläche; anschließend können Sie SuSE Linux das erste Mal ausprobieren.

3.3.8 Grafische Oberfläche vorbereiten

Um schon beim ersten *Einloggen* eine grafische Benutzeroberfläche zur Verfügung zu stellen, wird YaST2 nun versuchen, alle benötigten Informationen über den angeschlossenen Monitor und die Grafikkarte selbstständig herauszufinden.

Wenn dies gelingt, wird eine geeignete Bildschirmauflösung, Farbeinstellung und Wiederholfrequenz für den Monitor gewählt und der Testbildschirm angezeigt.



Hinweis

Bitte kontrollieren Sie die Einstellungen, bevor Sie Ihr ‘OK’ geben! Sehen Sie gegebenenfalls in den Unterlagen zur Grafikkarte und zu Ihrem Monitor nach.

Wird der Monitor nicht erkannt, dann wählen Sie Ihr Modell bitte aus der angezeigten Liste aus; besitzen Sie ein unbekanntes Modell, müssen Sie die Einstellungen von Hand eingeben oder die Daten von der ‘Treiber-Diskette’ einlesen lassen, die mit Ihrem Monitor mitgeliefert wurde; in jedem Fall sollten Sie die Dokumentation zu Ihrem Monitor zurate ziehen.

Stellen Sie die gewünschte Bildschirmauflösung und eine Farbtiefe von 16 bpp ein. Überprüfen Sie die Einstellungen, indem Sie ‘Test’ wählen, und und nehmen Sie bei Bedarf Feineinstellungen vor.

Tipp

In seltenen Fällen kann es notwendig sein, dass Sie den X-Server „von Hand“ konfigurieren müssen; dazu sollten Sie später das Programm SaX aufrufen.

Der standardmäßig verwendete Window-Manager auf dem SuSE Linux Adminhost for Firewall ist KDE2.

3.3.9 Netzwerk-Konfiguration mit YaST2

Für die Einrichtung des Netzwerks halten Sie bitte folgende Daten bereit: IP-Adresse, Netzwerkmaske, Default-Gateway.

Falls Sie einen DHCP-Server betreiben, können Sie den Adminhost auch als DHCP-Client konfigurieren. Es wird jedoch ausdrücklich empfohlen, eine feste IP-Adresse für den Adminhost zu vergeben. Sie bekommen eine Auswahl der von der Hardwareerkennung gefundenen Netzwerkkarten. Aktivieren Sie

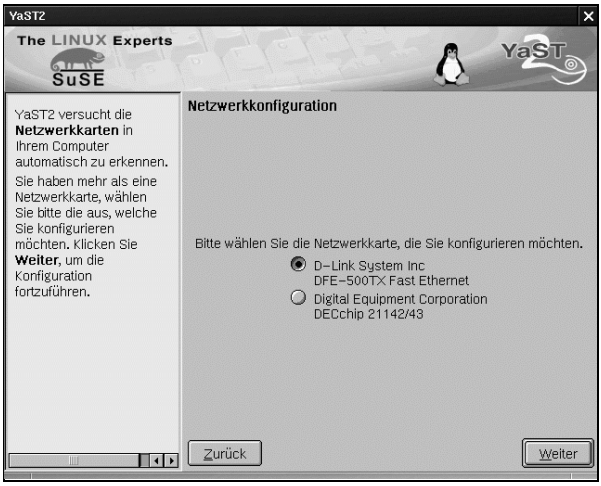


Abbildung 3.5: YaST2: Netzwerk-Konfiguration

die Netzwerkkarte und geben Sie die IP-Adresse und Netzwerkmaske ein. Tragen Sie alle notwendigen Angaben zu einem gegebenenfalls bereits bestehenden Nameserver wie in Abb. 3.7 auf der nächsten Seite ein.

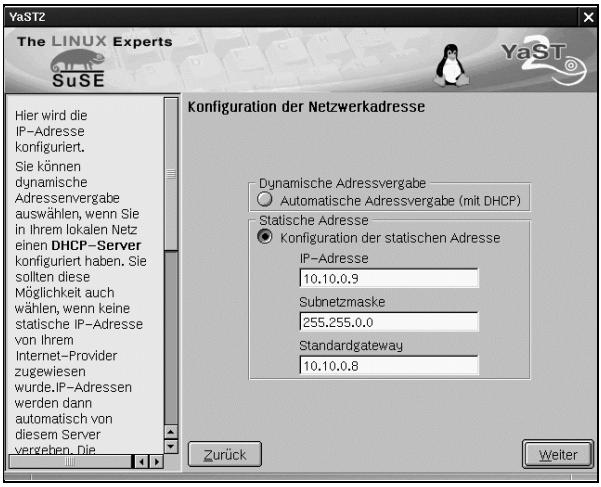


Abbildung 3.6: YaST2: Konfiguration der Netzwerkadresse

3.3.10 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte stets die zweite Wahl sein. Wir empfehlen, YaST zu benutzen, jedoch kann YaST nicht alle Bereiche der Netzwerkkonfiguration abdecken, so dass in manchen Fällen manuelle Nacharbeit nötig sein wird.

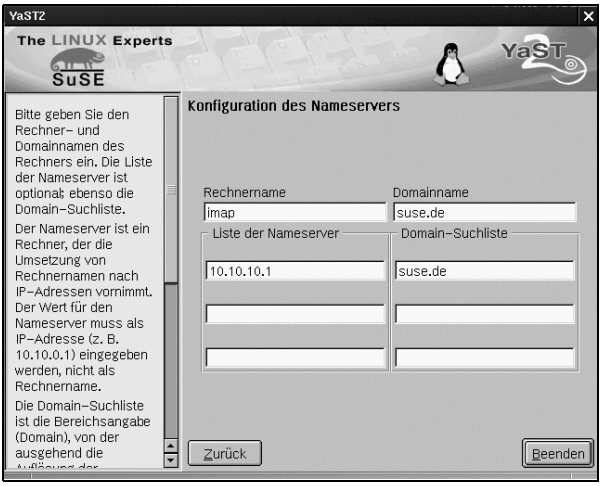


Abbildung 3.7: YaST2: Konfiguration des Nameservers

Konfigurationsdateien

Dieser Abschnitt gibt eine Übersicht über die Netzwerkkonfigurationsdateien und erklärt ihre Funktion sowie das verwendete Format.

`/etc/rc.config`
In dieser zentralen Konfigurationsdatei wird der größte Teil der Netzwerkkonfiguration vorgenommen. Bei Veränderung mittels YaST oder durch den Aufruf von SuSEconfig, nachdem die Datei manuell verändert wurde, werden aus diesen Einträgen die meisten der folgenden Dateien automatisch generiert. Auch die Bootskripten werden über die Einstellungen in dieser Datei konfiguriert.

Tipp
Wenn Sie diese Datei von Hand verändern, müssen Sie nachfolgend immer SuSEconfig aufrufen, damit die geänderte Konfiguration automatisch in die richtigen Dateien eingetragen wird.

`/etc/hosts`
In dieser Datei (siehe Datei 3.3.1 auf der nächsten Seite) werden Rechnernamen IP-Adressen zugeordnet. Wird kein Nameserver verwendet, so müssen hier alle Rechner aufgeführt werden, zu denen eine IP-Verbindung aufgebaut werden soll. Je Rechner wird eine Zeile bestehend aus IP-Adresse, dem voll qualifizierten Hostnamen und dem Rechnernamen, (z. B. `erde`) in die Datei eingetragen. Die IP-Adresse muss am Anfang der Zeile stehen, die Einträge werden durch Leerzeichen bzw. Tabulatoren getrennt. Kommentare werden durch `'#'` eingeleitet.

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.  Just add the names, addresses
#               and any aliases to this file...
#
127.0.0.1 localhost
192.168.0.1 sonne.kosmos.all sonne
192.168.0.20 erde.kosmos.all erde
# End of hosts
```

Datei 3.3.1: `/etc/hosts`

`/etc/networks`
Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen (siehe Datei 3.3.2).

```
#
# networks    This file describes a number of netname-to-address
#             mappings for the TCP/IP subsystem.  It is mostly
#             used at boot time, when no name servers are running.
#
loopback      127.0.0.0
localnet      192.168.0.0
# End of networks.
```

Datei 3.3.2: `/etc/networks`

`/etc/host.conf`
Das Auflösen von Namen – d. h. das Übersetzen von Rechner- bzw. Netzwerknamen über die *resolver*-Bibliothek – wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die gegen die libc4 oder die libc5 gelinkt sind; für aktuelle glibc-Programme vgl. die Einstellungen in `/etc/nsswitch.conf`! Ein Parameter muss in einer eigenen Zeile stehen, Kommentare werden durch `'#'` eingeleitet. Die möglichen Parameter zeigt Tabelle 3.1 auf der nächsten Seite.

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente sind (durch Leerzeichen oder Kommata voneinander getrennt): *hosts*: Durchsuchen der Datei `/etc/hosts` *bind*: Ansprechen eines Nameservers *nis*: Über NIS
multi *on*/*off*	Bestimmt, ob ein in `/etc/hosts` eingetragener Rechner mehrere IP-Adressen haben darf.

Tabelle 3.1: Fortsetzung auf der nächsten Seite...

nospoof *on* alert *on*/*off*	Diese Parameter beeinflussen das *spoofing* des Nameservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration.
trim <domainname>	Der angegebene Domainname wird vor dem Auflösen des Rechnernamens von diesem abgeschnitten (insofern der Rechnername diesen Domainnamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domain stehen, diese aber auch mit angehängtem Domainnamen erkannt werden sollen.

Tabelle 3.1: Parameter für `/etc/host.conf`

Ein Beispiel für `/etc/host.conf` zeigt Datei 3.3.3.

```
#
# /etc/host.conf
#
# We have named running
order hosts bind
# Allow multiple addrs
multi on
# End of host.conf
```

Datei 3.3.3: `/etc/host.conf`

`/etc/nsswitch.conf`

Mit der GNU C Library 2.0 hat der „Name Service Switch“ (NSS) Einzug gehalten (vgl. Manual-Page von **`nsswitch.conf`** (**`man 5 nsswitch.conf`**), sowie ausführlicher *The GNU C Library Reference Manual*, Kap. "System Databases and Name Service Switch"; vgl. Paket `libcinfo`, Serie `doc`).

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` zeigt Datei 3.3.4 auf Seite 32. Kommentare werden durch `'#'` eingeleitet. Dort bedeutet z. B. der Eintrag bei der „Datenbank“ `hosts`, dass nach `/etc/hosts` (`files`) eine Anfrage über DNS (vgl. Abschnitt A auf Seite 123) losgeschickt wird.

Die über NSS verfügbaren „Datenbanken“ sind in Tabelle 3.2 auf der nächsten Seite genannt. Zusätzlich sind in Zukunft `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten.

`aliases`	Mail-Aliase, von `sendmail`(8) verwendet; vgl. Manual-Page von **`aliases`** (**`man 5 aliases`**).

Tabelle 3.2: Fortsetzung auf der nächsten Seite...

`ethers`	Ethernet-Adressen.
`group`	Für Benutzergruppen, von `getgrent`(3) verwendet; vgl. Manual-Page von **`group`** (**`man 5 group`**).
`hosts`	Für Hostnamen und IP-Adressen, von `gethostbyname`(3) und ähnlichen Funktionen verwendet.
`netgroup`	Im Netzwerk gültige Liste von Hosts und Benutzern, um Zugriffsrechte zu steuern; vgl. Manual-Page von **`netgroup`** (**`man 5 netgroup`**).
`networks`	Netzwerknamen und -adressen, von `getnetent`(3) verwendet.
`passwd`	Benutzerpasswörter, von `getpwent`(3) verwendet; vgl. Manual-Page von **`passwd`** (**`man 5 passwd`**).
`protocols`	Netzwerk-Protokolle, von `getprotoent`(3) verwendet; vgl. Manual-Page von **`protocols`** (**`man 5 protocols`**).
`rpc`	„Remote Procedure Call“-Namen und -Adressen, von `getrpcbyname`(3) und ähnlichen Funktionen verwendet.
`services`	Netzwerkdienste, von `getservent`(3) verwendet.
`shadow`	„Shadow“-Passwörter der Benutzer, von `getspnam`(3) verwendet; vgl. Manual-Page von **`shadow`** (**`man 5 shadow`**).

Tabelle 3.2: Über `/etc/nsswitch.conf` verfügbare „Datenbanken“

Die Konfigurationsmöglichkeiten der NSS-„Datenbanken“ stehen in Tabelle 3.3.

`files`	direkt auf Dateien zugreifen, z. B. auf `/etc/aliases`.
`db`	über eine Datenbank zugreifen.
`nis` `nisplus`	NIS;
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar.
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar.
zusätzlich	ist es möglich, unterschiedliche Reaktionen bei bestimmten Lookup-Ergebnissen auszulösen; Details sind der Manual-Page von **`nsswitch.conf`** (**`man 5 nsswitch.conf`**) zu entnehmen.

Tabelle 3.3: Konfigurationsmöglichkeiten der NSS-„Datenbanken“

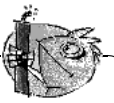
`/etc/nscd.conf`

```
#
# /etc/nsswitch.conf
#
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
```

Datei 3.3.4: `/etc/nsswitch.conf`

Über diese Datei wird der nscd (engl. *Name Service Cache Daemon*) konfiguriert (vgl. Manual-Page von **`nscd`** (**`man 8 nscd`**) und Manual-Page von **`nscd.conf`** (**`man 5 nscd.conf`**)). Betroffen sind die Informationen von `passwd`, `groups` und `hosts`. Der Daemon muss neu gestartet werden, wenn z. B. die Namensauflösung (DNS) durch Änderung der `/etc/resolv.conf` umgestellt wird. Dazu dient dieser Befehl:

```
erde: # rcnscd restart
```



Achtung

Wenn beispielsweise das Caching für `passwd` aktiviert ist, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten des nscd kann diese Wartezeit verkürzt werden.

`/etc/resolv.conf`

Wie bereits die Datei `/etc/host.conf`, so spielt auch diese Datei in Bezug auf Auflösung von Rechnernamen durch die *resolver*-Bibliothek eine Rolle.

In dieser Datei wird angegeben, welcher Domain der Rechner angehört (Schlüsselwort **`search`**) und wie die Adresse des Nameservers ist (Schlüsselwort **`nameserver`**), der angesprochen werden soll. Es können mehrere Domainnamen angegeben werden. Beim Auflösen eines nicht voll qualifizierten Namens wird versucht, durch Anhängen der einzelnen Einträge in **`search`** einen gültigen, voll qualifizierten Namen zu erzeugen. Mehrere Nameserver können durch mehrere Zeilen, die mit **`nameserver`** beginnen, bekannt gemacht werden. Kommentare werden wieder mit `'#'` eingeleitet.

Ein Beispiel für `/etc/resolv.conf` zeigt Datei 3.3.5 auf der nächsten Seite.

YaST trägt hier den angegebenen Nameserver ein!

```
# /etc/resolv.conf
#
# Our domain
search kosmos.all
#
# We use sonne (192.168.0.1) as nameserver
nameserver 192.168.0.1
# End of resolv.conf
```

Datei 3.3.5: `/etc/resolv.conf`

`/etc/HOSTNAME`
Hier steht der Name des Rechners, also nur der Hostname ohne den Domainnamen. Diese Datei wird von verschiedenen Skripten während des Starts des Rechners gelesen. Sie darf nur eine Zeile enthalten, in der der Rechnername steht! Auch diese Datei wird automatisch aus den Einstellungen in `/etc/rc.config` generiert.

Startup-Skripte

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die während des Hochfahrens des Rechners die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Multiuser-Runlevel* übergeht (vgl. Tabelle 3.4 auf der nächsten Seite).

`/etc/init.d/network`	Dieses Skript übernimmt die Konfiguration der Netzwerk Hard- und Software während der Startphase des Systems. Dabei werden auch die durch YaST in `/etc/rc.config` eingetragenen Angaben zu IP- und Netzwerk-Adresse, Netzmaske und Gateway ausgewertet.
`/etc/init.d/route`	Dient dem Setzen der statischen Routen im Netzwerk.
`/etc/init.d/inetd`	Startet den inetd, sofern es in `/etc/rc.config` festgelegt ist. Dies ist beispielsweise dann nötig, wenn Sie sich vom Netzwerk aus auf diese Maschine einloggen möchten.
`/etc/init.d/portmap`	Startet den Portmapper, der benötigt wird, um RPC-Server verwenden zu können, wie z. B. einen NFS-Server.
`/etc/init.d/nfsserver`	Startet den NFS-Server.
`/etc/init.d/sendmail`	Kontrolliert den sendmail-Prozess in Abhängigkeit von den Einstellungen in `/etc/rc.config`.

Tabelle 3.4: Fortsetzung auf der nächsten Seite...

`/etc/init.d/ypserv`	Startet den NIS-Server in Abhängigkeit von den Einstellungen in `/etc/rc.config`.
`/etc/init.d/ypbind`	Startet den NIS-Client in Abhängigkeit von den Einstellungen in `/etc/rc.config`.

Tabelle 3.4: Einige Startup-Skripten der Netzwerkprogramme

Bitte beachten Sie, dass der Hostname erst nach einem Neustart des Systems geschrieben wird. Einige Anwendungen funktionieren erst mit dem endgültigen Hostnamen.

3.3.11 Benutzer ‘`fwadmin`’ für das Firewall Administration System (FAS)

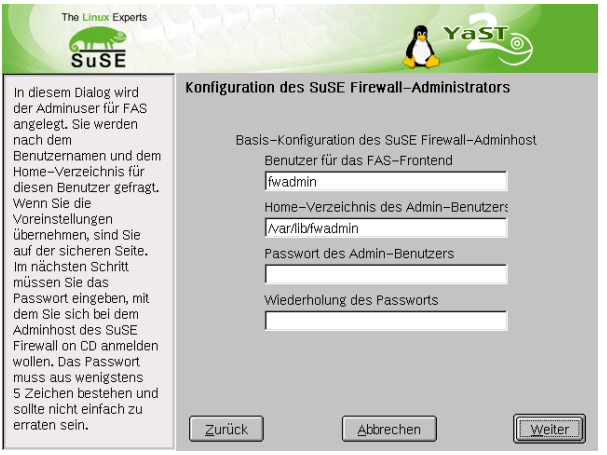


Abbildung 3.8: Benutzer für das Firewall Administration System (FAS)

In der Konfigurationsmaske ‘`Konfiguration des Admin-Benutzers für Firewall`’ (siehe Abbildung 3.8) richten Sie einen Benutzer ein, mit dem Sie die Konfiguration der SuSE Firewall CD vornehmen. Geben Sie einen Benutzernamen an, die Vorbelegung ist ‘`fwadmin`’. Weiterhin können Sie ein Home-Verzeichnis für den Benutzer angeben. Hier ist die Vorbelegung `/var/lib/fwadmin`. In dieser Konfigurationsmaske vergeben Sie dann das Passwort für den Admin-Benutzer der Firewall. Dieses Passwort besteht aus mindestens fünf Zeichen.

Im nächsten Screen müssen Sie zusätzlich eine „Passphrase“ definieren und im nächsten Feld wiederholen (siehe Abbildung 3.9 auf der nächsten Seite).

Damit wird die Grundinstallation des SuSE Linux Adminhost for Firewall abgeschlossen. Sie können am Bildschirm den Fortschritt mitverfolgen und erhalten am Ende die Erfolgsmeldung wie in Abbildung 3.10 auf der nächsten Seite.

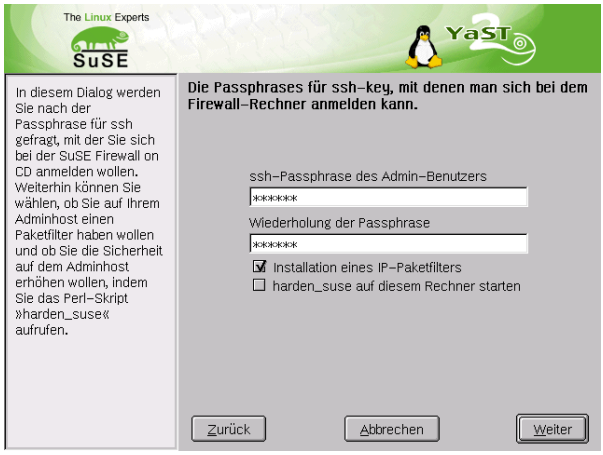


Abbildung 3.9: SSH-Passphrase für Admin-Benutzer definieren

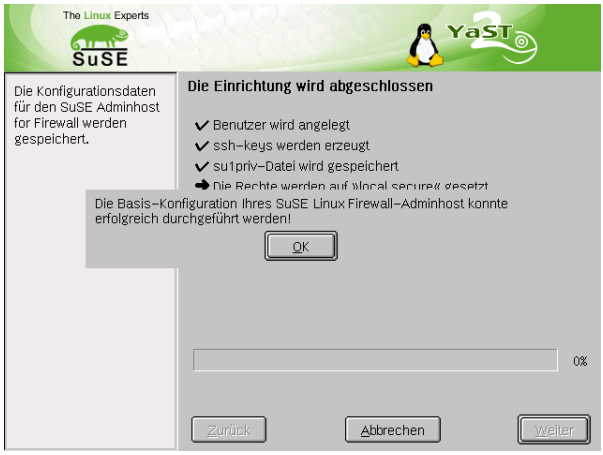


Abbildung 3.10: Abschluss der Installation

4 Firewall Administration System (FAS)

Nach der Installation bootet das System bis zum graphischen Login. Hier melden Sie sich als Benutzer `'fwadmin'` mit dem entsprechenden Passwort an. FAS funktioniert allerdings erst nach dem Neustart des Systems.

4.1 Einloggen als `'fwadmin'`

Sie gelangen auf den Desktop des Benutzers `'fwadmin'`, auf dem sich ein Icon befindet, mit dem Sie direkt die Administrations-Oberfläche für die Konfiguration der Live-CD starten (vgl. Abbildung 4.1).

Abbildung 4.1: FAS-Icon

4.2 Starten des Firewall Administration System

FAS ist die grafische Administrationsoberfläche, mit der Sie die Konfigurationsdiskette für die „SuSE Firewall CD“ erstellen. FAS unterstützt mehrere Benutzer und ist in der Lage, mehrere Konfigurationen zu verwalten.

Es handelt es sich um ein Client-Server-System, das aus der GUI und dem fasd Serverdaemon besteht. Der fasd (fas-daemon) managt die verschiedenen Konfigurationen, nimmt die Änderungen vor und prüft die Eingaben auf Richtigkeit. Das Frontend nimmt die Benutzerdaten entgegen und leitet sie an den Server weiter. Die Kommunikation zwischen Front- und Backend findet in dieser Version über Unix Domain Sockets statt.

Es gibt verschiedene Möglichkeiten, das Firewall Administration System zu starten:

1. Icon auf Desktop (vgl. Abbildung 4.1),
2. Auswahl aus dem K-Menü,
3. Geben Sie an der Kommandozeile (z. B. xterm) den Befehl **FAS** ein.

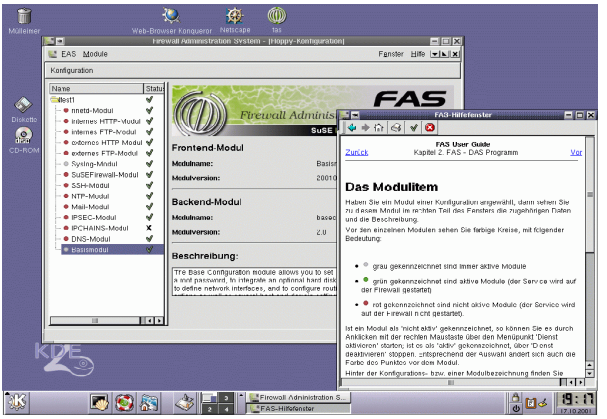


Abbildung 4.2: Desktop mit FAS und Hilfefenster

4.3 Erstellen einer neuen Firewall-Konfiguration

Nachdem Sie das Konfigurationsprogramm FAS gestartet haben, müssen Sie einen neuen Benutzer-Account in FAS anlegen. Dazu wählen Sie im Menü ‘FAS’ den Menüpunkt ‘`Login anlegen`’ aus. Es folgt ein Dialog, in dem Sie einen neuen Benutzernamen und ein Passwort vergeben. Der Benutzername muss mindestens fünf Zeichen lang sein. Das Passwort muss zwischen fünf und acht Zeichen lang sein. Mit diesem Passwort schützen Sie die Konfiguration der „SuSE Firewall on CD“, deshalb wird dieses Passwort mit dem Programm cracklib auf seine Tauglichkeit überprüft.

Allgemein gilt: Gute Passwörter sind nicht zu erraten, also bitte nicht das eigene Geburtsdatum, den Straßennamen oder den Namen des Lieblingsstars etc. verwenden. Sie sollten nicht zu kurz sein und dennoch schnell zu tippen, damit Sie niemand bei der Eingabe beobachten kann. Verwenden Sie Groß- und Kleinbuchstaben und Zahlen gemischt. Natürlich ist es bei alledem wichtig, dass man sich ein Passwort auch merken kann und es nicht aufschreiben muss. Eine bewährte Methode der Passwortfindung sind daher Abkürzungen von Sätzen oder Ausdrücken, die man sich leicht einprägen kann. Hier einige Beispiele:

- NE14TenS (anyone for tennis?)
- AuaEGC (all UNIX-admins eat green cheese)
- A10imGt (Am Zehnten ist mein Geburtstag)
- Iw,ihegP (Ich wünschte, ich hätte ein gutes Passwort)

Die Konfiguration der „SuSE Firewall on CD“ wird in einem `.tar.gz`-Archiv abgespeichert. Um eine bereits erstellte Konfiguration bearbeiten zu können, müssen Sie dieses Passwort wieder angeben.

Nach der Anmeldung wählen Sie im Menü ‘`Konfiguration`’ den Punkt ‘`Neue Konfiguration`’ aus. Es erscheint ein neues Fenster, in dem Sie einen Namen

für die Konfiguration festlegen. Weiterhin müssen Sie eine Beschreibung der Konfiguration eingeben. Diese Beschreibung kann dazu benutzt werden, den Zweck der Konfiguration zu erläutern und zu dokumentieren, wer, wann, was an der Konfiguration geändert hat. Die Beschreibung der Konfiguration kann später jederzeit erweitert oder verändert werden. Nutzen Sie diese Möglichkeit, gute Dokumentation ist wichtig.

Bestätigen Sie mit ‘OK’.

Sie sehen jetzt den Namen Ihrer neuen Konfiguration im linken Fenster. Wenn Sie einmal auf den Namen klicken, wird rechts die Beschreibung der Konfiguration angezeigt. Sie können jetzt die Beschreibung editieren. Um Änderungen an der Konfigurationsbeschreibung zu speichern, klicken Sie auf ‘Änderungen speichern’. Klicken Sie zweimal kurz hintereinander (Doppelklick) auf den Namen Ihrer Konfiguration, um mit der Erstellung der Konfiguration zu beginnen.

In der linken Fensterhälfte wird eine Liste mit den Konfigurations-Modulen, d. h. mit den Diensten, die Sie für Ihre Firewall konfigurieren können, und der Status, in dem sich das jeweilige Modul befindet, angezeigt. Als erstes müssen Sie die Basis-Module (‘Basismodul’ und ‘Syslogmodul’) konfigurieren. Solange sich diese Module im Zustand „nicht konfiguriert“ (symbolisiert durch ein Kreuz) befinden, ist es nicht möglich, eines der anderen Module auszuwählen.

Die Dienste werden durch Anklicken mit der rechten Maustaste und Auswählen von ‘Dienst aktivieren’ in der Firewall-Konfiguration aktiviert. Dies wird durch einen grünen Punkt symbolisiert. Das Basis-Modul und Syslog-Modul sind immer aktiv.

Liste der verfügbaren Module:

- Basismodul (Netzwerkinterfaces, Hostname, Rootpasswort)
- DNS Modul (Nameserver)
- External ftp (Konfiguration des ftp-Proxies von Extern nach Intern/DMZ)
- External http (Konfiguration des Http-Proxies von Extern nach Intern/DMZ)
- IPCHAINS-Modul (Import eines selbstgenerierten ipchains Regelsatzes)
- IPSEC Modul (Konfiguration von IPsec-Tunneln)
- Internal ftp
- Internal http
- Mail Modul
- NTP Modul (Konfiguration von xntpd zum Abgleich der Rechnerzeit mit einem Zeitserver)
- SSH Modul
- SuSE Firewall Modul (Erstellen eines Paketfilters mit dem SuSE Firewall Skript)
- Syslog Modul (Konfiguration des syslogd auf der Firewall)
- rinetd Modul (Konfiguration des generischen tcp-Proxies rinetd)

4.3.1 Konfiguration des Basismoduls

Diese Grundkonfiguration der Firewall erfolgt in fünf Schritten:

1. `'root'`-Passwort für die Firewall:

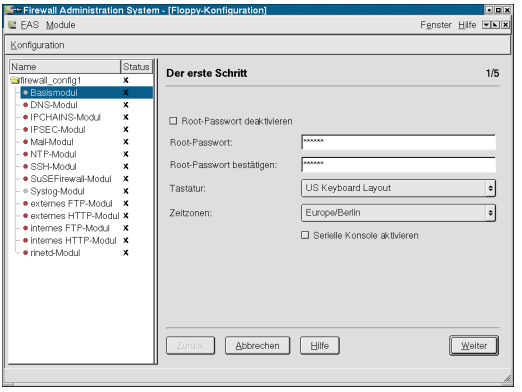


Abbildung 4.3: Root-Passwort festlegen

In diesem Dialog (vgl. Abbildung 4.3) wird das `'root'`-Passwort für die Firewall gesetzt. Wenn Sie kein `'root'`-Passwort vergeben (Checkbox deaktivieren), kann sich im späteren Betrieb niemand direkt auf dem Firewall-Rechner als `'root'` anmelden. Es ist nur noch der Zugang via ssh und RSA-Schlüssel möglich, falls Sie ssh konfigurieren.

'`Serielle Konsole aktivieren`' ermöglicht den Anschluss einer seriellen Konsole, von der aus man die Firewall steuern kann.

2. Setup der (optionalen) Festplatte (vgl. Abbildung 4.4):

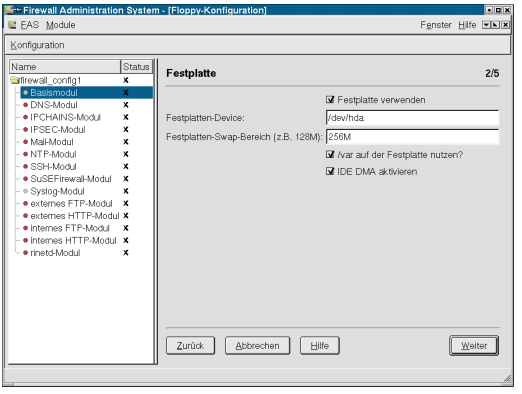


Abbildung 4.4: Festplatten-Setup

Wenn Sie ‘`Festplatte verwenden`’ aktivieren, können Sie folgende Einstellungen vornehmen:

Festplatten-Device: Angabe der Festplatte, die eingebunden werden soll: z. B.: `/dev/hda` (1. Festplatte am 1. IDE-Controller)

Festplatten-Swap-Bereich: Größe der Swap-Partition: z. B. 128 MB

Checkbox ‘`/var auf der Festplatte nutzen?`’ Soll das Verzeichnis `/var` auf dem Festplatten-Device liegen?

IDE DMA aktivieren: aktiviert DMA für IDE

Wenn Sie den E-Mail-Proxy verwenden und/oder das Caching beim HTTP-Proxy aktivieren und/oder die Log-Meldungen auf der Festplatte speichern wollen, muss die Festplatte konfiguriert und /var aktiviert sein.

3. Netzwerk-Interfaces (vgl. Abbildung 4.5):

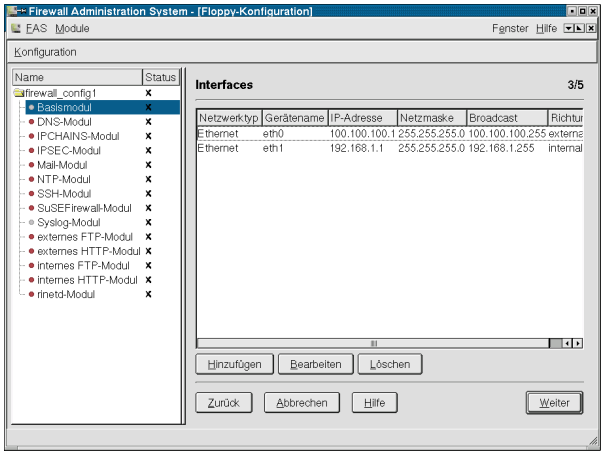


Abbildung 4.5: Netzwerk-Interfaces

Falls Sie schon Netzwerkschnittstellen konfiguriert haben, finden Sie in diesem Dialog eine Liste mit bereits angelegten Interfaces. Es können maximal zehn Interfaces angegeben werden, wobei mindestens ein internes und ein externes eingetragen werden müssen. Mit ‘`Hinzufügen`’ wird ein neues Netzwerkinterface angelegt. Es erscheint ein Fenster mit dem ‘`Interface-Dialog`’ (vgl. Abbildung 4.6 auf der nächsten Seite). Folgende Angaben sind notwendig:

Netzwerktyp: Ethernet ist „default“ (in dieser Version wird nur Ethernet unterstützt).

Gerätename: Wird automatisch fortlaufend vergeben.

IP-Adresse: IP-Adresse, die dem Interface zugewiesen werden soll.

Netzmaske: Die Netzmaske zur IP-Adresse.

Richtung: intern/extern; ist das Interface am Intranet, an der DMZ oder am Internet angeschlossen?

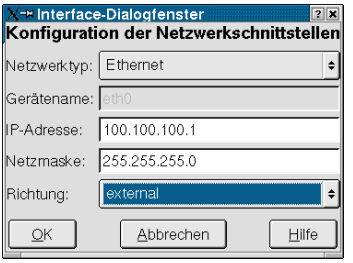


Abbildung 4.6: Neues Netzwerkinterface anlegen

Mit ‘OK’ bestätigen Sie die Einstellungen, mit ‘Abbrechen’ können Sie den Dialog abbrechen. Das neu konfigurierte Interface taucht jetzt in der Liste auf. Mit ‘Bearbeiten’ lässt sich ein vorhandenes Interface umkonfigurieren. Suchen Sie ein Interface aus der Liste aus und wählen Sie ‘Bearbeiten’. ‘Löschen’ entfernt das ausgewählte Interface.

4. Routing (vgl. Abbildung 4.7)

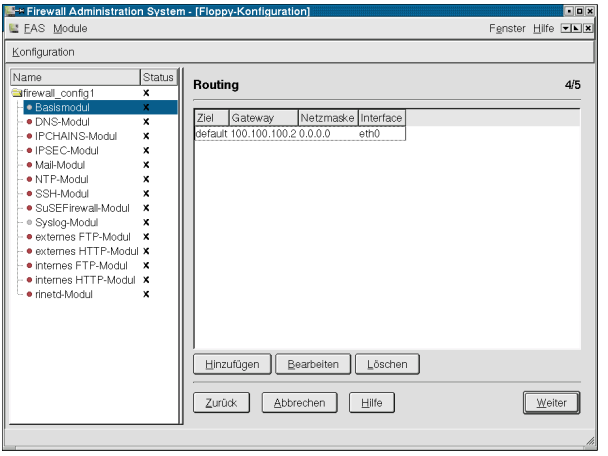


Abbildung 4.7: Routing-Konfiguration

Hier können Sie explizit Routen setzen. ‘Hinzufügen’ erstellt eine neue Route, mit ‘Bearbeiten’ verändern Sie eine bestehende Route.

In der Dialogbox ‘Routing konfigurieren’ (vgl. Abbildung 4.8 auf der nächsten Seite) können folgende Einstellungen vorgenommen werden:

Ziel: In welches Netz bzw. zu welchem Host soll geroutet werden? Geben Sie die Netzwerkadresse ein (z. B. 192.168.0.0).

Gateway: Ist ein Gateway nötig, welche IP-Adresse hat es?

Netzmaske: Die zugehörige Netzwerkmaske.

Interface: Über welches Interface soll die Route laufen?

Abbildung 4.8: Routing

Wie zuvor speichern Sie die Einstellungen mit ‘`OK`’ und brechen die Konfiguration mit ‘`Abbrechen`’ ab. Mit ‘`Löschen`’ entfernen Sie eine bestehenden Route.

5. Host- und Domain-Konfiguration (vgl. Abbildung 4.9):

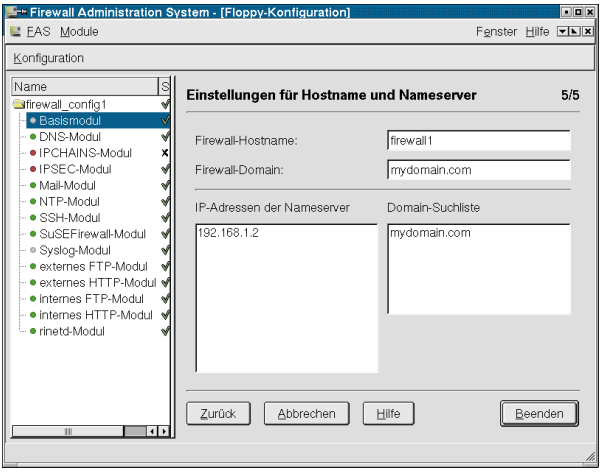


Abbildung 4.9: Host- und Domain-Konfiguration

Firewall-Hostname: Geben Sie den Namen des Firewall-Rechners an. Vermeiden Sie Namen wie: Gateway oder Firewall.

Firewall-Domain: Geben Sie den Namen der Domain an, zu der die Firewall gehört.

Nameserver: Um den Resolver richtig zu konfigurieren, geben Sie hier Ihre Nameserver an und die Searchlisten, z. B. `your-company-inc.com`.

4.3.2 Syslog-Konfiguration:

In diesem Dialog (vgl. Abbildung 4.10) können Sie das Verhalten des Syslog-Daemons konfigurieren. Sie haben die Möglichkeit, die Ausgabe des syslogd auf die Festplatte und zusätzlich oder auch ausschließlich auf einen Log-Host zu legen. Geben Sie eine Liste von IP-Adressen von Rechnern an, auf denen die Logs geschrieben werden sollen. Diese Rechner müssen entsprechend konfiguriert werden, damit sie die logs auch entgegennehmen können. Der SuSE Linux Firewall Adminhost ist für diese Aufgaben bereits vorbereitet.

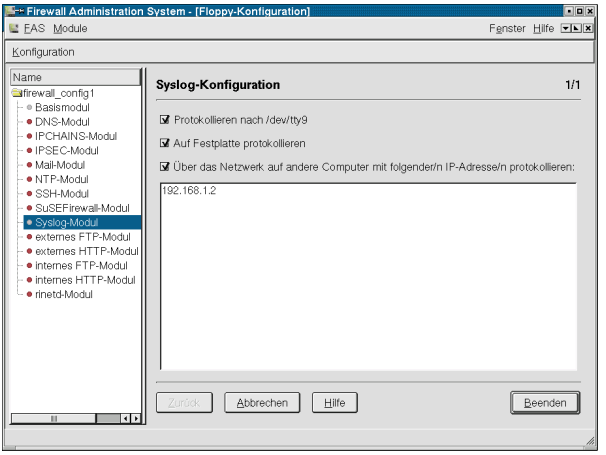


Abbildung 4.10: Syslog-Konfiguration

Die Konfiguration des syslog-ng auf dem SuSE Firewall Adminhost wird im Abschnitt 4.8 auf Seite 79 erklärt.

4.3.3 DNS-Konfiguration

In diesem Menü wird das Nameserver-bind8 konfiguriert. Ausführliche Erklärungen zu DNS und bind8 finden Sie im Anhang dieses Handbuchs.

DNS Forwarder IP-Adressen: Hier geben Sie an, ob Sie DNS-Anfragen an einen oder mehrere andere Nameserver weitergeben wollen. Dazu schalten Sie die CheckBox ‘`DNS Forwarder IP-Adressen`’ ein. Daraufhin wird die Listenbox aktiviert. Jetzt können Sie eine Liste von Nameservern angeben, an die DNS-Anfragen weitergeleitet werden sollen. Wenn Sie die Checkbox ‘`Nur an Forwarder weiterleiten`’ aktivieren, werden die Anfragen ausschließlich an diese Nameserver weitergeleitet. Ist sie deaktiviert, werden auch die so genannten „root“-Nameserver (allgemein bekannte Nameserver im Internet) gefragt (vgl. Abbildung 4.11 auf der nächsten Seite).

Höre auf ausgewählte IP-Adresse(n): Der bind8-Nameserver nimmt standardmäßig auf allen Netzwerk-Interfaces, die zur Verfügung stehen, Anfragen

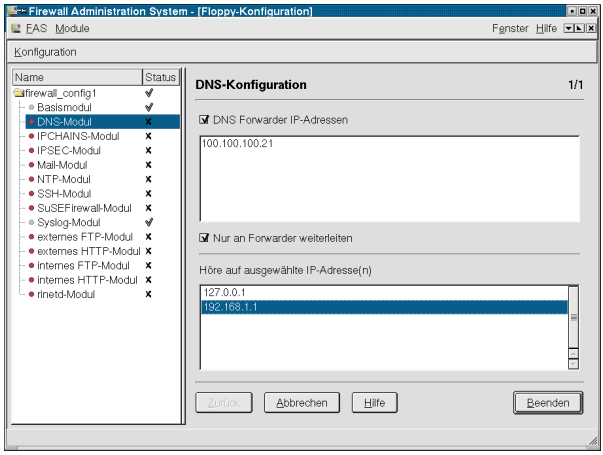


Abbildung 4.11: DNS-Konfiguration

entgegen, also sowohl auf den internen als auch auf den externen Netzwerk-Interfaces und dem Loopback-Interface. Wählen Sie in der Listenbox die Interfaces aus, auf denen DNS-Anfragen angenommen werden dürfen.

4.3.4 IP Filter Konfiguration mit ipchains

Im FAS ipchains-Modul (vgl. Abbildung 4.12) geben Sie eine Datei an, in der Sie mit **`ipchains-save`** eine Paketfilter-Konfiguration abgespeichert haben (siehe auch **`man 8 ipchains-save`**). Diese Datei wird eingelesen und später auf der Konfigurationsdiskette abgelegt.

Diese Konfiguration können Sie so ganz einfach auf die Firewall übernehmen.

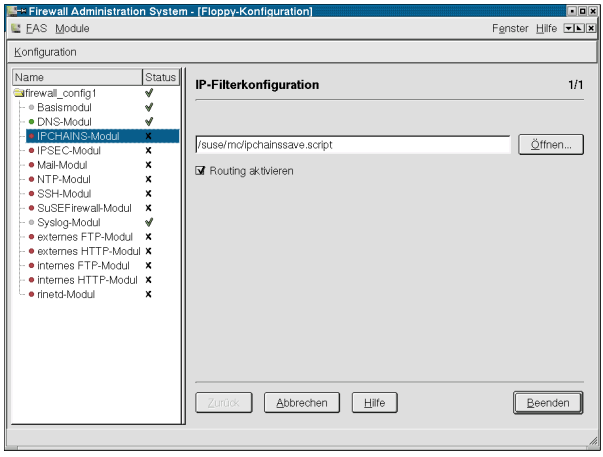


Abbildung 4.12: IP-Paketfilter-Konfiguration mit ipchains

4.3.5 Konfiguration des SuSE Firewall Moduls

Mit diesem Modul konfigurieren Sie Schritt für Schritt das SuSE Firewall-Skript.

1. Im ersten Schritt geben Sie an, welches der von Ihnen im Basis-Modul konfigurierten Netzwerk-Interfaces für die DMZ (Demilitarisierte Zone) bzw. Ihr internes Netz vorgesehen ist. Hier erscheinen diejenigen, die von Ihnen in der Basis-Konfiguration als interne Netzwerk-Interfaces gekennzeichnet wurden. Wählen Sie per Mausklick aus der Liste aus (vgl. Abbildung 4.13). Diejenigen, die von Ihnen im Basis-Modul als externe Interfaces gekennzeichnet wurden, erscheinen hier automatisch im Textfeld „Internet-Device“.

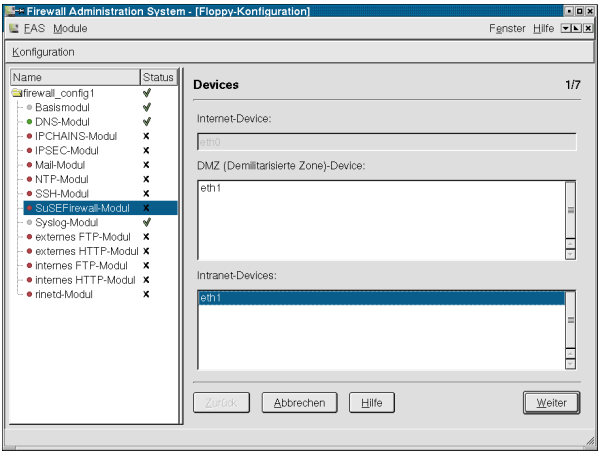


Abbildung 4.13: Devices auswählen

2. Routing Filter: Hier können Sie das direkte Routen von IP-Paketen erlauben, indem Sie eine Quell- und eine Ziel-Adresse sowie einen Zielport angeben (vgl. Abbildung 4.14 auf der nächsten Seite). Dies benötigen Sie für Dienste ohne Proxies. Weiterhin können Sie in diesem Dialog angeben, ob Sie Masquerading verwenden wollen. Dies kann notwendig sein, wenn Sie von Ihrem Internet Service Provider nur eine oder eine geringe Anzahl offizieller IP-Adressen zugewiesen bekommen haben und Ihre Rechner im internen Netz Adressen aus den sog. privaten IP-Adressbereichen benutzen. Dazu aktivieren Sie die Checkbox Masquerading für die entsprechende Verbindung.

   Um IPsec Verbindungen durch die Firewall zu routen, wählen Sie aus der Combobox ‘`Protokoll`’ den Eintrag ‘`50`’ aus. (Die 50 bezieht sich auf die für die IPSEC-Familie verwendete Portnummer). Hinweis: Sie müssen auch den Port isakmp / udp für diese Verbindungen durch die Firewall „routen“.

3. Umleitung: Um transparentes „proxying“ zu ermöglichen, müssen Sie Pakete umleiten. Sie wollen beispielsweise den internen HTTP-Proxy transparent konfigurieren. Die IP-Pakete haben als Quell-Adresse eine interne IP-Adresse und als Ziel-Adresse eine IP-Adresse des Internets. Als Zielport haben diese IP-Pakete Port 80 (www). Ihr HTTP-Proxy erwartet aber die

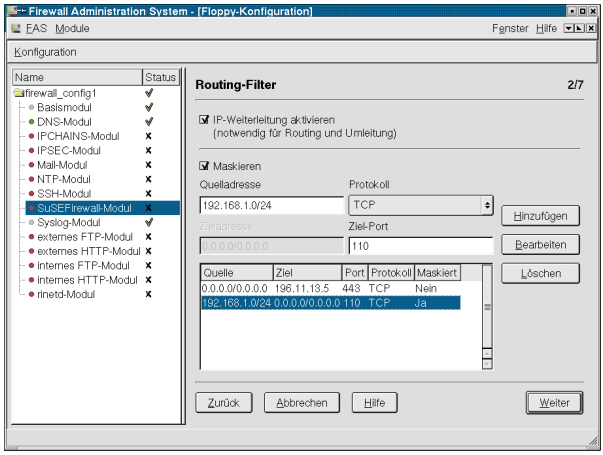


Abbildung 4.14: Routing-Filter

Pakete auf ihrer Firewall auf dem Port 3128. Diese Umleitung von einer Zieladresse mit Zielport 80 auf localhost Port 3128, die hier erforderlich ist, kann in dieser Maske konfiguriert werden (vgl. Abbildung 4.15).

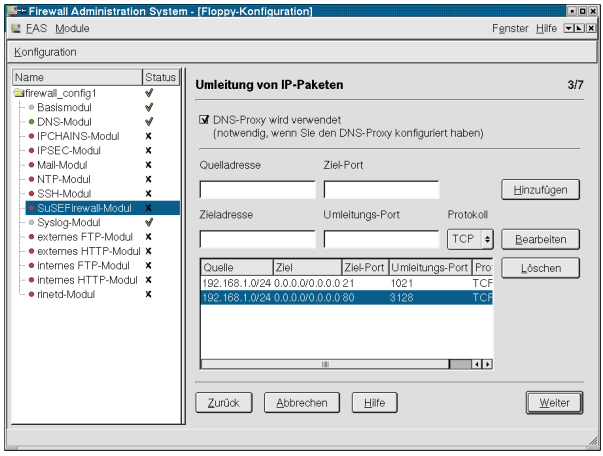


Abbildung 4.15: Umleitung von Paketen

4. Freischalten von Ports für internen Zugang zur Firewall. Welche Dienste der Firewall wollen Sie für das interne Netz zur Verfügung stellen? Wählen Sie aus der angebotenen Liste (vgl. Abbildung 4.16 auf der nächsten Seite). Checkbox: Erlaube IPSec Verbindung von Intern. Diese Checkbox muss aktiviert werden, wenn Sie einen VPN-Tunnel aus dem internen Netz auf den Firewall-Rechner aufbauen wollen.

5. Ports Freischalten von extern auf die Firewall: Wählen Sie aus der Liste die Ports aus, die Sie dafür freigeben wollen, das heißt, die vom Internet aus

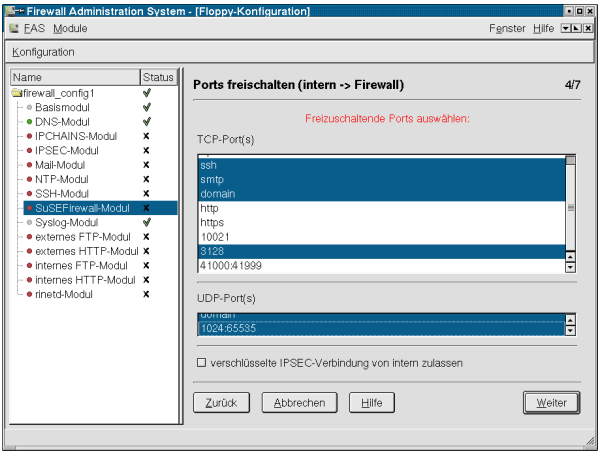


Abbildung 4.16: Ports freischalten von intern zur Firewall

zugänglich sein sollen (vgl. Abbildung 4.17).

Checkbox: Erlaube IPSec Verbindung von Extern. Diese Checkbox muss aktiviert werden, wenn Sie einen VPN-Tunnel aus dem Internet auf den Firewall-Rechner aufbauen wollen.

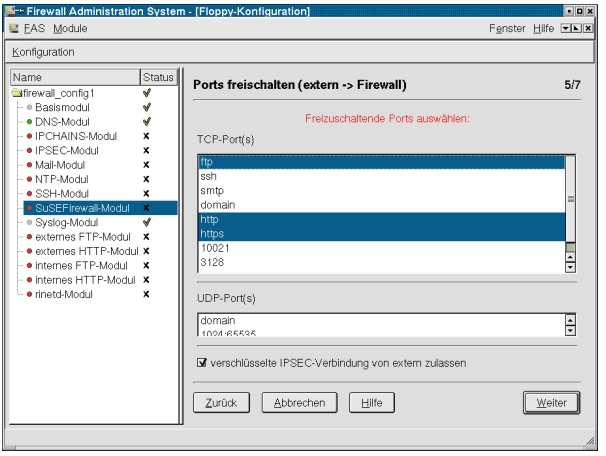


Abbildung 4.17: Ports freischalten von extern zur Firewall

6. Schalten Sie die Ports frei, die von der DMZ aus die Firewall erreichen sollen, indem Sie wiederum aus der angezeigten Liste wählen (vgl. Abbildung 4.18 auf der nächsten Seite). (Wenn bei 1.) keine DMZ-Interfaces gewählt wurden, ist dieser Bildschirm deaktiviert.)

   Checkbox: Erlaube IPSec Verbindung von DMZ. Diese Checkbox muss aktiviert werden, wenn Sie einen VPN-Tunnel aus der DMZ auf den Firewall-Rechner aufbauen wollen.

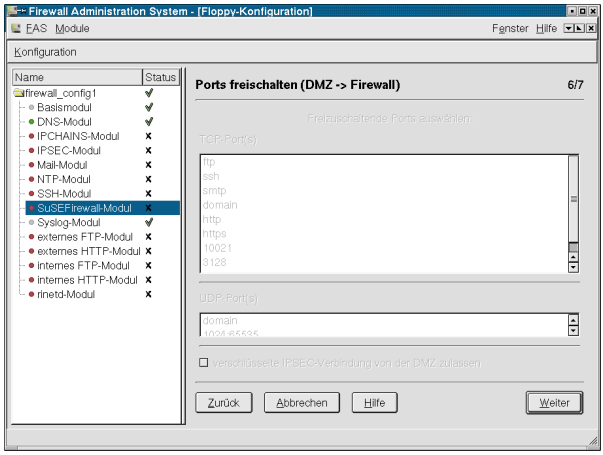


Abbildung 4.18: Ports freischalten von der DMZ zur Firewall

7. Protokoll und Kernelmodule.

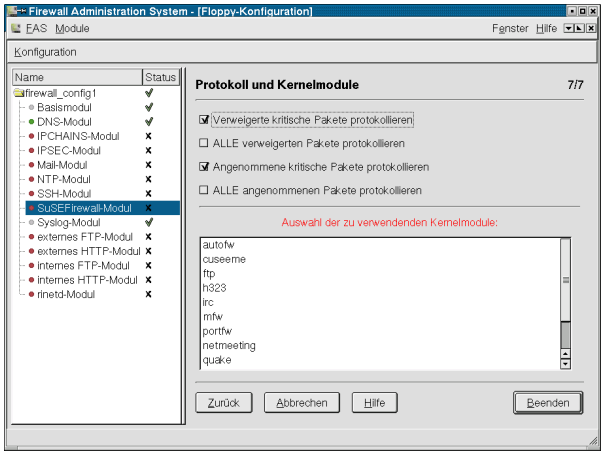


Abbildung 4.19: Auswahl von Protokoll- und Kernelmodulen

- Aus der Reihe von Checkboxen wählen Sie den „Loglevel“ für den Paketfilter. Beachten Sie dabei bitte, dass die Logfiles sehr schnell anwachsen können, wenn Sie alle Pakete mitloggen.
- Im Auswahlfeld der Kernelmodule wählen Sie die Module aus, die Sie benötigen, wenn Sie bestimmte Anwendungen über die Firewall hinweg verwenden (vgl. Abbildung 4.19).

4.3.6 Konfiguration des Mail-Relays (Postfix)

Um dieses Modul verwenden zu können, müssen Sie in der Basis-Konfiguration eine Festplatte eingebunden haben.

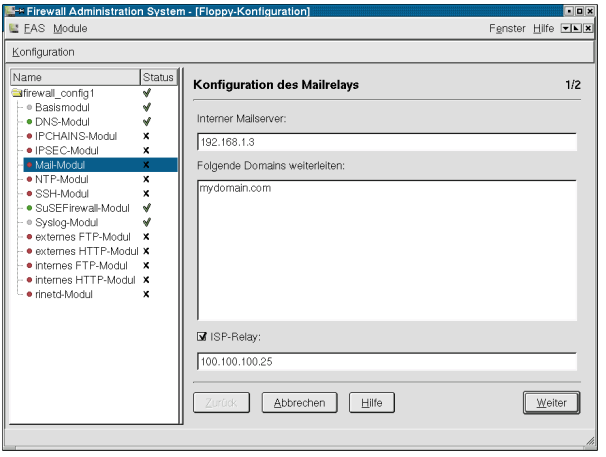


Abbildung 4.20: Konfiguration des Mail-Relays – Dialog 1

Interner Mailserver: Geben Sie die IP-Adresse oder den Namen Ihres internen Mail-Servers an (vgl. Abbildung 4.20).

Checkbox ISP-Relay: Aktivieren Sie diese Checkbox, wenn Sie alle ausgehenden E-Mails an den SMTP-Server Ihres Internet-Service-Providers (ISP) weiterleiten. Geben Sie den Namen (FQHN) oder die IP-Adresse des SMTP-Servers Ihres Providers an.

Folgende Domains weiterleiten: Hier tragen Sie die Domain-Namen ein, die vom Mail-Relay entgegengenommen und an den Mailserver weitergeleitet werden sollen.

Lokale Netzwerke: Liste Ihrer Netzwerke. Postfix entscheidet anhand dieser, ob ein Netzwerk E-Mails über die Firewall versenden darf. Geben Sie hier Ihre Netzwerke ein (z. B. `192.168.0.0/24`) (vgl. Abbildung 4.21 auf der nächsten Seite).

Höre auf ausgewählte IP-Adressen: Geben Sie hier die IP-Adressen an, auf denen das Mail-Relay Anfragen entgegennimmt.

4.3.7 SSH-Konfiguration:

SSH-Keys: Hier haben Sie die Möglichkeit Ihren „ssh-public-key“ für den Zugang als `'root'` auf der Firewall zu hinterlegen, damit Sie sich auf dem Firewall-Rechner einloggen können. Sie haben zwei Möglichkeiten (vgl. Abbildung 4.22 auf der nächsten Seite):

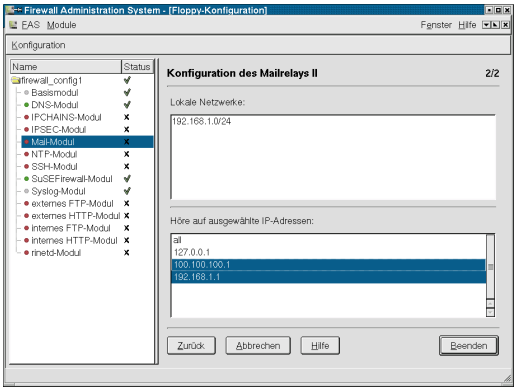


Abbildung 4.21: Konfiguration des Mail-Relays – Dialog 2

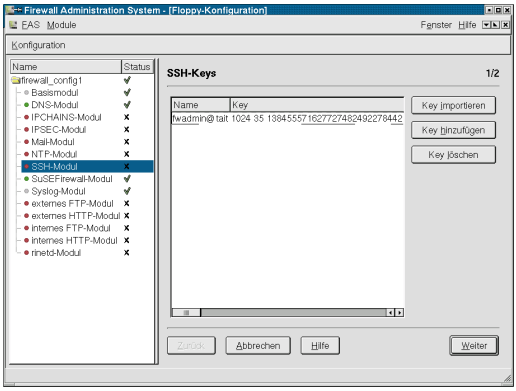


Abbildung 4.22: SSH-Keys hinzufügen bzw. löschen

- Sie können einen Key importieren. Ein „ssh-key“ liegt normalerweise im Home-Verzeichnis des Benutzers im Verzeichnis `.ssh/` in der Datei `identity.pub` . Wählen Sie diese Datei aus. Der Schlüssel erscheint dann in der Liste (vgl. Abbildung 4.23 auf der nächsten Seite).
- Sie können einen Key auch mittels „copy&paste“ eintragen. Wenn Sie auf ‘`Key hinzufügen`’ klicken, wird ein Dialog geöffnet (vgl. Abbildung 4.24 auf der nächsten Seite). Im Textfeld können Sie Ihren „ssh-public-key“ angeben und mit ‘`OK`’ bestätigen. Dieser Schlüssel taucht jetzt in der unteren Liste auf.

Key löschen: Wählen Sie den zu löschenden Schlüssel aus. Klicken Sie auf ‘`Key löschen`’. Der ausgewählte Schlüssel wird entfernt.

Checkbox Greife auf Passwort-Authentifizierung zurück: Wenn Sie dies aktivieren (vgl. Abbildung 4.25 auf der nächsten Seite), wird ein Einloggen per Passwort auf der Firewall ermöglicht. Wir raten Ihnen dringend, nur Zugang per RSA-Schlüssel zu erlauben.

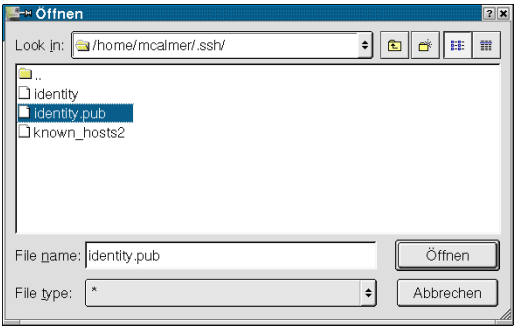


Abbildung 4.23: Key importieren

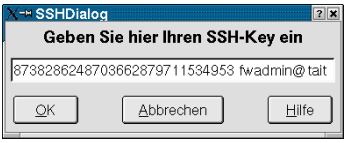


Abbildung 4.24: Key hinzufügen

Höre auf ausgewählte IP-Adresse: Auf welchem Netzwerkinterface soll ssh Anfragen entgegennehmen? Geben Sie die IP-Adressen in das Listenfeld ein.

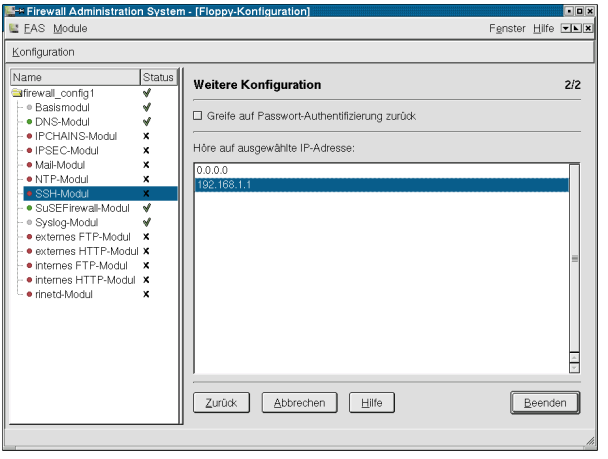


Abbildung 4.25: SSH-Konfiguration

4.3.8 Ftp-Zugang von extern nach intern:

Wenn Sie einen eigenen FTP-Server betreiben, müssen Sie hier folgende Einstellungen vornehmen (vgl. Abbildung 4.26 auf der nächsten Seite):

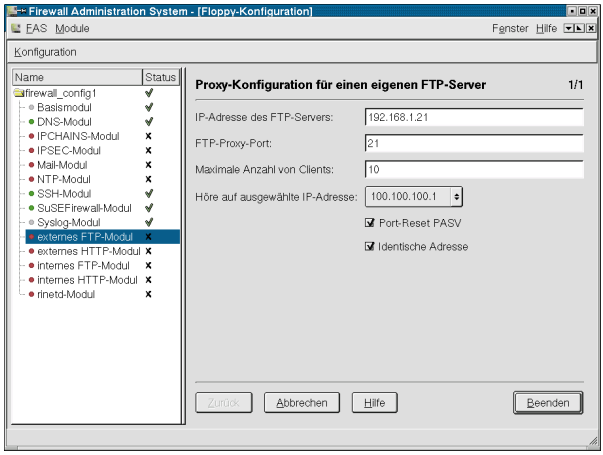


Abbildung 4.26: Konfiguration des FTP-Servers

IP-Adresse des FTP-Servers: Die IP-Adresse Ihres FTP-Servers, der in Ihrem Intranet bzw. der DMZ steht.

FTP-Proxy-Port: Der Port, auf dem Ihr FTP-Server horcht, normalerweise ist das Port 21. Damit wird, von außen betrachtet, Ihre Firewall zum FTP-Server. Lassen Sie sich von Ihrem Provider für Ihre Firewall einen Alias-Eintrag im DNS geben, z. B.: `ftp.mycompany.com`

Maximale Anzahl von Clients: Maximale Anzahl an FTP-Clients, die sich gleichzeitig mit dem FTP-Server verbinden dürfen.

Höre auf ausgewählte IP-Adresse: IP-Adresse des Interfaces, auf dem der FTP-Server Verbindungen entgegen nimmt.

4.3.9 Konfiguration des FTP-Proxies von intern nach extern:

FTP-Proxy-Port: 10021
Port, auf dem der FTP-Proxy angesprochen wird.

Magic User: Wenn Sie diese Checkbox aktivieren, wird im Benutzernamen der ausgewählte Ziel-FTP-Server angegeben: user[@host[:port]]. Das sieht dann zum Beispiel so aus:

```
> ftp user@remoteftp.remote.org:21
```

Magic Char: Das MagicChar-Zeichen ist standardmäßig auf „%“ eingestellt. Wenn die Option ‘`Magic User`’ aktiviert ist, kann das Zeichen beliebig gewählt werden.

Maximal Clients: Maximale Anzahl an offenen Verbindungen auf den FTP-Proxy.

Höre auf ausgewählte IP-Adresse: IP-Adresse, über die der FTP-Proxy angesprochen wird.

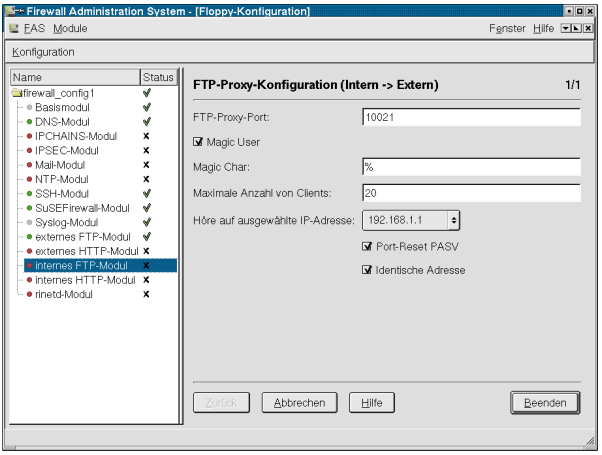


Abbildung 4.27: Konfiguration des FTP-Proxies

4.3.10 Konfiguration des HTTP-Proxys für Verbindungen von intern nach extern

In diesem Modul können Sie die Einstellungen zum HTTP-Proxy vornehmen. Dieser bearbeitet die HTTP-Anfragen von Benutzern des internen Netzes.

HTTP-Proxy

Zur Konfiguration des HTTP-Proxies sind folgende Einträge notwendig:

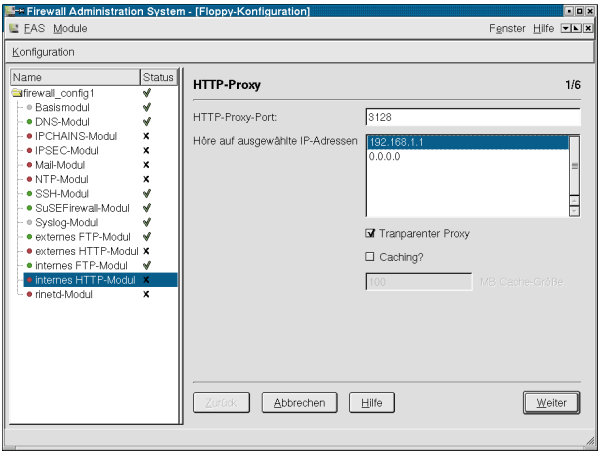


Abbildung 4.28: Konfiguration des HTTP-Proxies – Dialog 1

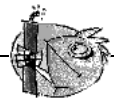
HTTP-Proxy-Port Der Port, auf dem der Proxy die HTTP-Anfragen von intern entgegen nehmen soll. Standardeinstellung ist Port `3128` (vgl. Abbil-

dung 4.28 auf der vorherigen Seite).

Höre auf ausgewählte IP-Adressen Hier legen Sie die IP-Adresse der Firewall fest, von der HTTP-Anfragen entgegen genommen werden dürfen. In der Auswahlliste finden Sie die Interfaces, die in der Basiskonfiguration als intern gekennzeichnet wurden. 0.0.0.0 steht für alle Interfaces der Firewall.

Transparenter Proxy Grundsätzlich überwacht der Proxy nur den Port 3128. Wenn eine HTTP-Anfrage gestellt wird, läuft diese über Port 80 und wird nicht bearbeitet. Um diese Anfrage zu bearbeiten, muss die Option '`Transparenter Proxy`' aktiviert sein. Damit verbunden muss eine „Redirect"-Regel (Umleitung) existieren, die die Anfrage innerhalb der Firewall auf den Port 3128 umleitet. Wenn Sie diese Option nicht aktivieren, müssen alle Clients oder der interne Proxy die Firewall als Proxy eingetragen haben.

Caching Wiederholen sich HTTP-Anfragen, so können Sie die Option '`Caching?`' aktivieren, um ein wiederholtes Abarbeiten von gültigen Seiten zu vermeiden. Die Größe des Cache können Sie im zugeordneten Eingabefeld bestimmen und sollte nicht unter 100 MB liegen.



Achtung

Die Firewall sollte nicht als zwischenspeichender HTTP-Proxy verwendet werden, da darin nicht die eigentliche Aufgabe besteht. Eine bessere Lösung ist der Einsatz eines zusätzlichen eigenständigen Rechners.

Haben Sie alle Veränderungen vorgenommen, bestätigen Sie die Einstellungen mit '`Weiter`'.

ACLs definieren

Hier legen Sie fest, wer den Proxy verwenden darf und auf was diese Benutzer im Internet zugreifen können (vgl. Abbildung 4.29 auf der nächsten Seite).

Name für ACL Vergeben Sie zunächst einen Namen für die anzulegende Liste.

Typ der ACL Als Nächstes wählen Sie einen '`Typ`' für Ihre ACL. Sie haben die Wahl zwischen:

url_regex Angabe von URL-Adressen.

proto (protocol) Hier legen Sie die entsprechenden Protokolle fest.

src (source) Bestimmung der Quelladressen.

dst (destination) Angabe der Zieladressen.

Hinzufügen Fügen Sie die neue ACL der Liste von bereits angelegten ACLs hinzu.

Löschen Sie können ACLs über diese Schaltfläche auch wieder löschen.

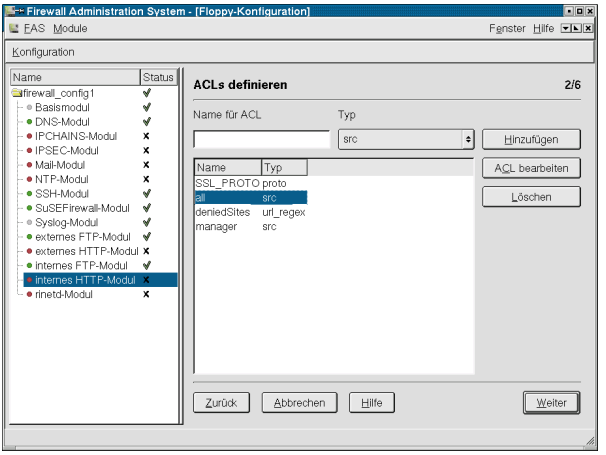


Abbildung 4.29: Konfiguration des HTTP-Proxies – Dialog 2

ACL bearbeiten In diesem Fenster können Sie Werte eintragen bzw. ändern, die für eine von Ihnen ausgewählte ACL gelten sollen. Sie können in das Eingabefeld neue Werte hinzufügen bzw. bestehende Werte editieren oder löschen.

Haben Sie alle Veränderungen vorgenommen, bestätigen Sie die Einstellungen mit ‘`Weiter`’.

ACLs anordnen

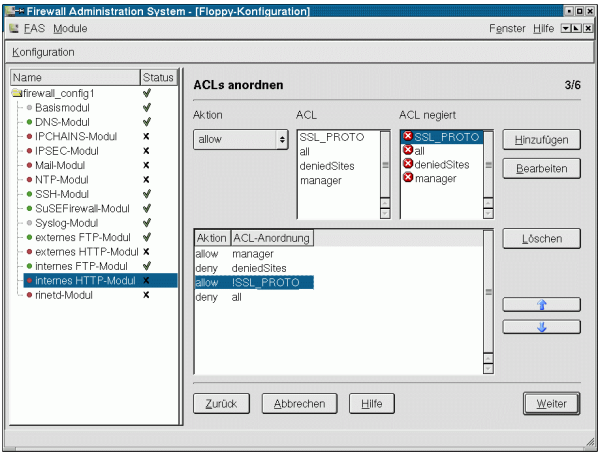
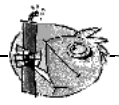


Abbildung 4.30: Konfiguration des HTTP-Proxies – Dialog 3

Zum Einrichten der Regeln (ACL) finden Sie auf dieser Modulseite verschiedene Möglichkeiten. Die ausgewählten Einstellungen bei ‘`ACL`’ und ‘`ACL negiert`’ im oberen Teil werden „UND“-verknüpft (vgl. Abbildung 4.30).

- Mit dem ‘Aktion’-Auswahlfeld wählen Sie zwischen ‘allow’ zum Erlauben bzw. ‘deny’ zum Verbieten der Internetzugriffe, die Sie im nachfolgenden festlegen werden.
- Bestimmen Sie über ‘ACL’ eine bereits angelegte Liste, für die die Einstellungen gültig werden.
- Bestimmen Sie über ‘Negate ACL’ eine ACL, die negiert eingesetzt werden soll. So können Sie z. B. das Abrufen von Internetseiten erlauben (Auswahl bei ‘ACL’), die aber nicht über SSL-Ports laufen (Auswahl bei ‘Negate ACL’).
- Eine neue Regel binden Sie über ‘Hinzufügen’ ein.
- Zum Editieren von Regeln, klicken Sie die entsprechende im Listenfeld an. Daraufhin werden die Einstellungen im oberen Teil übernommen. Sie können diese nun verändern und mit ‘Bearbeiten’ übernehmen.
- Zum Löschen von Regeln wählen Sie die entsprechende aus und klicken auf ‘Löschen’.
- Im unteren Teil des Fensters finden Sie eine Listenfeld, in dem alle Aktionen und zugehörigen ACL-Einstellungen eingetragen sind.



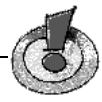
Achtung

Die Reihenfolge der Regeln im Listenfeld ist sehr wichtig, denn die aufgestellte Liste wird von oben nach unten abgearbeitet. Je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben oder gesperrt.

- Um eine Regel um eine Stelle zu verschieben, wählen Sie die entsprechende Regel aus und aktivieren Sie im rechten Rand des Fensters zum Verschieben nach unten die Schaltfläche mit dem blauen Pfeil nach unten; zum Verschieben nach oben die Schaltfläche mit dem blauen Pfeil nach oben.
- Haben Sie alle Veränderungen vorgenommen, bestätigen Sie die Einstellungen mit ‘Weiter’.

Content Filter

Um HTML Seiteninhalte zu filtern bzw. nach bestimmten Seiteninhalten zu durchsuchen und evtl. Inhalte zu sperren, aktivieren Sie die Checkbox bei ‘Content Filter’ (vgl. Abbildung 4.31 auf der nächsten Seite).



Hinweis

Sie sollten HTML programmieren können, um diesen Filter zu konfigurieren. Die „Tags“ und „Attribute“, von denen im Folgenden die Rede ist, sind Komponenten aus HTML, der Beschreibungssprache, in der Webseiten geschrieben sind.

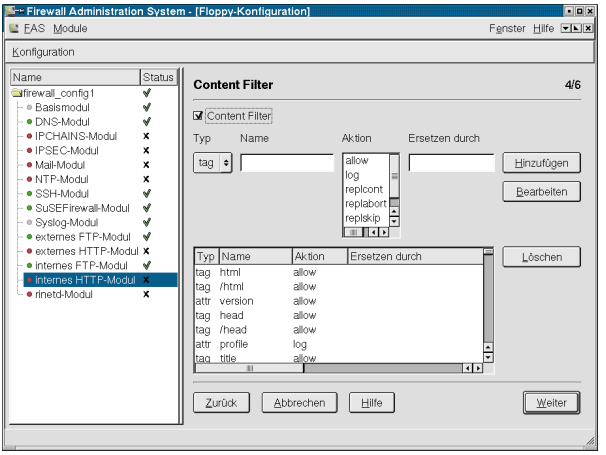


Abbildung 4.31: Konfiguration des HTTP-Proxies – Dialog 4

Alle angelegten Filtereinstellungen finden Sie im unteren Teil des Fensters. Dort sind Typen Namen zugewiesen, Aktionen definiert und Ersetzungen angegeben. Beachten Sie bitte, dass jedes HTML-Tag oder Attribut, das nicht definiert ist, abgelehnt wird.

Gehen Sie bitte folgendermaßen vor:

- Zum Anlegen einer Filterregel wählen Sie den entsprechenden Typ aus dem gleichnamigen Auswahlfeld. Zur Wahl stehen Ihnen ‘`tag`’ und ‘`attr`’ für Attribut. Im Eingabefeld ‘`Name`’ geben Sie den Text des „Tags“ oder „Attributs“ an und wählen anschließend eine Aktion aus. Mehrfachnennung von Aktionen ist möglich. Zur Wahl stehen Ihnen:

  allow erlaubt das ausgewählte Tag/Attribut.

  log setzt einen Eintrag ins so genannte „log-file“ und kann später für das Erstellen von Filterstrategien genutzt werden.

  replcont ersetzt das Tag/Attribut und das Auswerten der Attribute wird fortgesetzt.

  replabort ersetzt das Tag/Attribut und das Auswerten der Attribute wird abgebrochen.

- Um ganze Code-Teile aus den angeforderten Dokumenten zu entfernen, dienen folgende zwei Aktionen:

  replskip zeigt den Beginn einer Auslassung an, die nicht an den Benutzer weitergeleitet wird.

  replendskip zeigt das Ende der Auslassung an.

- In dem Eingabefeld bei ‘`Ersetzen durch`’ geben Sie die Zeichenkette ein, die an Stelle der zu ersetzenden Zeichenkette eingesetzt werden soll. Es sind keine Leerstellen erlaubt. Zum Einfügen von Leerstellen nutzen Sie `&#32;`. Hier etwas einzufügen macht natürlich nur Sinn, wenn Sie als Aktion ‘`replcont`’, ‘`replabort`’, ‘`replskip`’ oder ‘`replendskip`’ gewählt haben.

- Zum Editieren einer Filterregel wählen Sie diese aus dem Listenfeld aus. Die Werte werden Ihnen daraufhin in den Eingabe- und Auswahlfeldern im oberen Bereich des Fensters angezeigt. Modifizieren Sie die Werte und bestätigen Sie durch Anklicken von ‘`Bearbeiten`’.
- Zum Löschen von Filterregeln, wählen Sie diese aus dem Listenfeld aus und aktivieren Sie ‘`Löschen`’.

MIME Type Filter

Einführung

Das Contentfiltering auf der SuSE Linux Firewall on CD erfolgt durch den httpf-Proxy.

Ein Teil des Content-Filterings wird durch die auf einer HTML-Seite enthaltenen Tags angestossen.

Content Filtering kann an Hand der sog. MIME-Types der via http abgerufenen Dokumente aus dem WWW erfolgen. Zu diesen MIME-Types gehören z. B. Bilder (GIF, JPEG, . . .), Audiodateien, (MPEG, WAV, . . .) oder Videos (MPEG, AVI, . . .).

Anhand des übertragenen Bit-Streams lässt sich feststellen, zu welcher Art MIME-Type das angeforderte Dokument gehört.

Es ist somit möglich, entsprechende Dateien zu erkennen und entweder die Übertragung zu erlauben oder zu unterbinden.

Wenn httpf einen MIME-Type erkennt, der nicht definiert ist, dann wird das entsprechende Objekt nicht durchgelassen.

Damit wird es außerdem möglich, festzustellen, ob der übertragene MIME-Type mit dem übertragenen Inhalt übereinstimmmt und nicht zum Beispiel ein ausführbares Programm sich als „harmloses“ gif-Bild ausgibt.

Um das Contentfiltering zu konfigurieren, steht in FAS auf dem „SuSE Adminhost for Firewall CD“ ein MIME-Type Editor zur Verfügung.

Die erzeugte Konfiguration wird dann zusammen mit der übrigen Firewall- Konfiguration auf die Konfigurationsdiskette geschrieben.

Bedienung

Das Fenster Filter für Mime-Typ zeigt in einer Liste alle schon konfigurierten MIME-Types an (vgl. Abbildung 4.32 auf der nächsten Seite).

Die drei Felder ‘`MIME-Typ`’, ‘`Offset`’ und ‘`Zeichenkette`’ dienen zur Neuanlage eines Types bzw. dazu, einen Mime-Type zu editieren.

‘`MIME-Typ`’ gibt an, um welchen MIME-Type es sich handelt. Offset bezeichnet die Stelle nach Dateianfang, an der sich der String „Zeichenkette“ befindet.

Die beiden Parameter ‘`Offset`’ und ‘`Zeichenkette`’ sind optional, da nicht alle Dateiformate eindeutig zu erkennen sind.

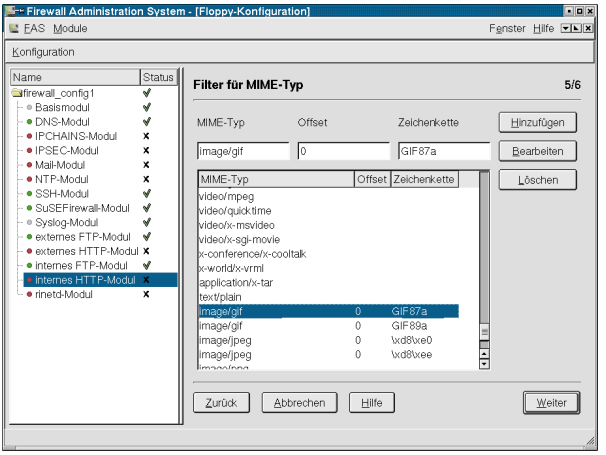


Abbildung 4.32: Konfiguration des HTTP-Proxies – Dialog 5

Alle MIME-Types, die durch den Mimetype/Contentfilter gelangen sollen, müssen in diesem Interface definiert sein.

Eine Konfiguration mit den meisten MIME-Types ist im Default-Template enthalten.

Parent-Proxy-Konfiguration

Sollte Ihr Provider für HTTP-Anfragen einen bestimmten Proxy zur Verfügung stellen, so kann die IP-Adresse des Proxies im Eingabefeld bei ‘`IP-Adresse des Parent-Proxies`’ eingetragen werden. Der zugehörige HTTP-Port des Providers wird bei ‘`Parent-Proxy-Port`’ eingetragen (vgl. Abbildung 4.33 auf der nächsten Seite).

Ist der ‘`Content Filter`’ nicht aktiviert, können Sie bei ‘`Parent-Proxy-ICP-Port`’ (ICP = Internet Caching Protocol) den ICP-Port des Providers angeben, wenn dessen Proxy ICP unterstützt.

Haben Sie alle Veränderungen vorgenommen, bestätigen Sie die Einstellungen mit ‘`Beenden`’.

4.3.11 Konfiguration des HTTP-Proxies für Verbindungen von extern nach intern

Wenn Sie keinen eigenen Web-Server betreiben, müssen Sie hier nichts konfigurieren. Ansonsten nehmen Sie bitte folgende Einstellungen vor (vgl. Abbildung 4.34 auf Seite 62):

HTTP-Proxy-Port: Der Port, auf dem der Proxy lauscht. Normalerweise ist das 80. Damit wird, von außen betrachtet, Ihre Firewall zum Web-Server. Lassen Sie sich also einen Alias für ihre Firewall von Ihrem Provider geben, z. B.: `www.my-company.com`

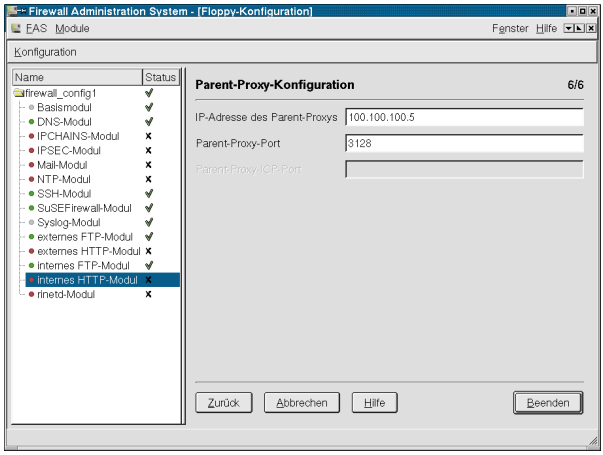


Abbildung 4.33: Konfiguration des HTTP-Proxies – Dialog 6

Höre auf ausgewählte IP-Adresse: IP-Adresse des Interfaces, auf dem der Proxy Verbindungen entgegen nimmt.

IP-Adresse des Webservers: Die IP-Adresse Ihres Web-Servers, der in Ihrem Intranet steht.

Webserver-Port: Normalerweise ist dies Port 80.

4.3.12 Das FAS Keyring Modul

Das „Keyring Modul“ in FAS wird benötigt, um die Zertifikate für die Verschlüsselung bei der Verwendung von IPsec mit X.509 Zertifikaten zu erzeugen, importieren und zu verwalten. Das Modul taucht nicht in der linken Modulliste auf, sondern ist in der oberen Menülesite über ‘`Module`’ → ‘`Zertifikat-Verwaltung`’ zu erreichen.

Über Zertifikate und Certificate Authority (CA):

Die Schlüssel und Zertifikate werden auf dem SuSE Adminhost for Firewall mit dem Programm-Paket OpenSSL erstellt.

SSL und PKI Mit SSL wird asymmetrisch verschlüsselt, d. h. es ist zur Verschlüsselung und Entschlüsselung immer ein Schlüsselpaar, bestehend aus Public- und Private-Key notwendig.

PKI - asymmetrische Verschlüsselung Bei diesem Verfahren werden die Public-Keys zwischen Client und Server ausgetauscht. Die Verschlüsselung erfolgt mit dem Public-Key der jeweiligen Seite.

Zur Entschlüsselung wird der Private Key benötigt.

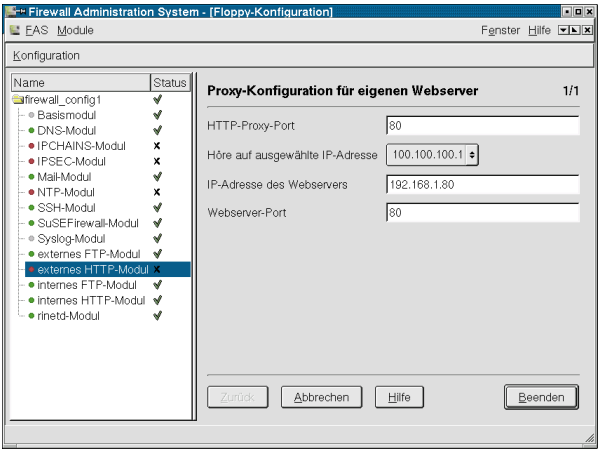


Abbildung 4.34: Konfiguration des externen HTTP-Proxies

CA Certificate Authority

Um ein Zertifikat zu signieren, benötigen Sie eine CA. Es gibt Stellen, die eine offizielle CA haben. Dieser Stelle müssen Sie jedes Ihrer Zertifikate zur Signierung übergeben.

Sie können sich aber auch eine CA selbst erzeugen und Ihre Zertifikate selbst signieren.

Dies ist für die meisten Zwecke vollkommen ausreichend.

X.509 Zertifikate

Ein X.509 Zertifikat besteht aus den folgenden Teilen:

- Version
- Serial
- Signieralgorithmus
- issuer-Name
- Gültigkeitsdauer
- Subject Username
- Subject Publickey Information
- issuer unique identifier
- subject unique identifier
- extensions
- signature on above

FAS stellt ein Frontend für die Erstellung von X.509 Zertifikaten zur Verfügung.

Zertifikat-Verwaltung

Starten Sie das FAS. Melden Sie sich im FAS als Adminbenutzer an.

Wählen Sie im Menü ‘`Module`’ den Punkt ‘`Zertifikat-Verwaltung`’.

Sie bekommen nun eine Liste angezeigt, in der, falls vorhanden, die schon vorhandenen Zertifikate angezeigt werden (Abbildung 4.35).

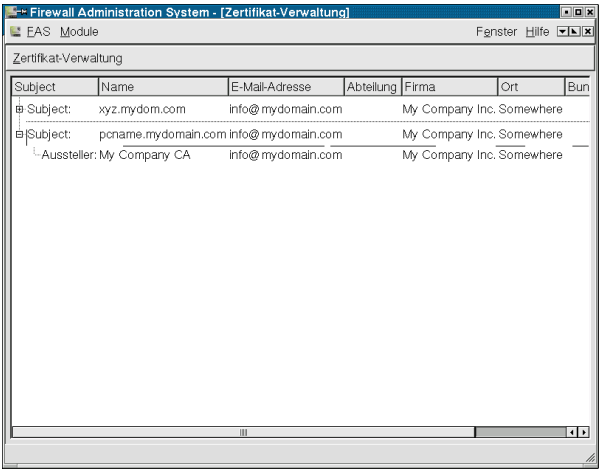


Abbildung 4.35: Liste der Zertifikate

Beim ersten Starten haben Sie normalerweise noch keine CA (Certificate Authority). Sie benötigen die CA, um Zertifikate für Ihre Clients zu erstellen.

CA erstellen

Diesen Dialog können Sie nur einmal aufrufen.

Diese CA ist global für alle Konfigurationen, die auf diesem Adminhost erstellt werden. Mit dieser CA werden alle Zertifikate, die Sie erstellen, signiert.

Starten Sie im Menü ‘`Zertifikat-Verwaltung`’ den Punkt ‘`CA erstellen`’. Es erscheint ein Dialog, den Sie vollständig ausfüllen sollten (Abb. 4.36 auf der nächsten Seite). Viele dieser Einstellungen werden für die Erzeugung von Clientzertifikaten übernommen.

- Zunächst benötigen Sie einen Namen für Ihre CA, z. B. Ihren Firmennamen.
- Unter E-Mail-Adresse geben Sie den für die CA verantwortlichen Mitarbeiter an. (z.B. Sicherheitsbeauftragter für Ihr Firmennetz)
- Abteilung: Geben Sie hier z. B. den Abteilungsnamen an.
- Firma: Ihr Firmenname
- Ort: Ort, z. B. Ihr Firmensitz

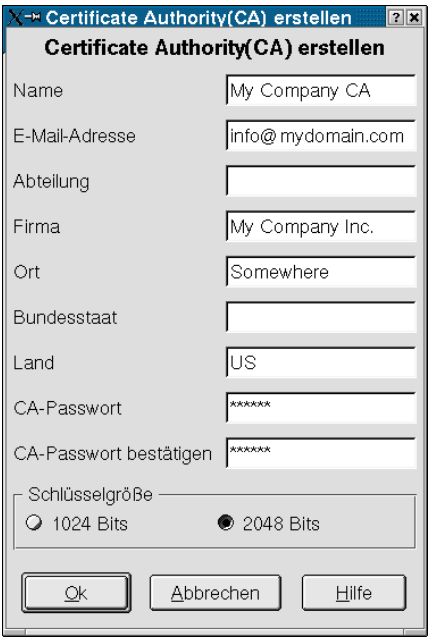


Abbildung 4.36: Dialog zur Erstellung einer CA

- Bundesstaat: Bundesland
- Land: Das zweibuchstabige Länderkürzel Ihres Landes (DE, US, usw.)
- CA-Passwort: Geben Sie ein Passwort für die CA an, um sie gegen Missbrauch zu schützen. Kontrolleingabe der Passphrase.
- Schlüsselgröße: Sie können hier die Schlüssellänge wählen. Ein längerer Schlüssel lässt sich schwerer „knacken“. Auswählen können Sie 1024 oder 2048 bit.

Nachdem Sie alle notwendigen Angaben gemacht haben, bestätigen Sie mit ‘`OK`’. Wenn die Erzeugung der Certificate Authority (CA) erfolgreich verlaufen ist, erhalten Sie eine Erfolgsmeldung.

Erstellen eines Zertifikates

Wählen Sie den Menüpunkt ‘`Zertifikat-Verwaltung`’ und den Unterpunkt ‘`Zertifikat erstellen`’. Es erscheint ein Dialogfenster, in dem Sie die notwendigen Angaben für ein neues Zertifikat eingeben können (Abb. 4.37 auf der nächsten Seite).

Zunächst geben Sie den Namen (cn) für das Zertifikat an, z. B. den Hostnamen des Rechners, für den das Zertifikat bestimmt ist.

Unter ‘`E-Mail-Addresse`’ geben Sie (falls nicht schon auf Grund der CA ausgefüllt) Ihre E-Mail-Adresse an.

Auch die folgenden Punkte sind vorausgefüllt, ansonsten füllen Sie sie analog der CA-Erstellung aus. Um das Zertifikat mit Ihrer CA zu signieren, benötigen Sie noch das Passwort für Ihre CA.

Ihr neu erstelltes Zertifikat sollte mit einem Passwort geschützt werden. Geben Sie das Passwort für Ihr neues Zertifikat ein und wiederholen Sie die Eingabe zur Kontrolle.

Nun wählen Sie noch die Grösse Ihres Schlüssels aus (Grundeinstellung ist 2048 Bits). Nachdem Sie alle notwendigen Eingaben gemacht haben, klicken Sie auf ‘OK’ Nach erfolgreicher Erstellung des Zertifikates erhalten Sie eine Erfolgsmeldung. Ihr neuerstelltes Zertifikat erscheint nun in der Liste.

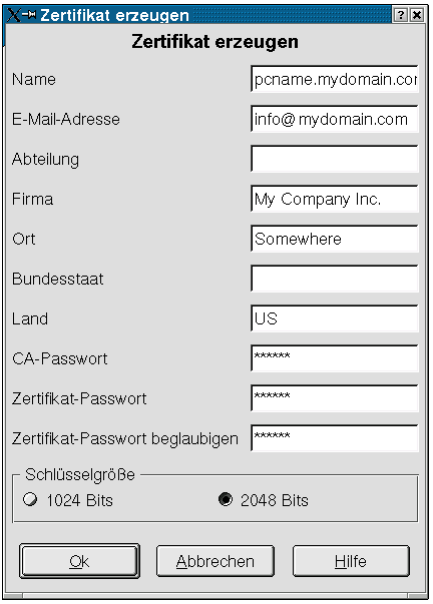


Abbildung 4.37: Dialog zur Erstellung eines Zertifikates

Löschen eines Zertifikates

Wählen Sie aus der Zertifikat-Liste ein Zertifikat aus, das Sie löschen (revoken) wollen.

Wählen Sie unter dem Menüpunkt ‘Zertifikat-Verwaltung’ den Eintrag ‘Zertifikat widerrufen’ aus. Sie werden aufgefordert, das Passwort für die CA einzugeben, mit der das Zertifikat erstellt wurde. Es erscheint eine Warnung, ob Sie das Zertifikat wirklich widerrufen wollen. Bestätigen Sie mit ‘Ja’. Es erscheint eine Erfolgsmeldung, dass das Zertifikat erfolgreich gelöscht wurde.

Die Liste der Zertifikate wird aktualisiert angezeigt.

Importieren von Zertifikaten

Klicken Sie im Menü ‘`Zertifikat-Verwaltung`’ auf ‘`Zertifikat importieren`’. Aus dem nun erscheinenden Verzeichnis-Listing wählen Sie die Datei aus, die das Zertifikat enthält.

Gültige Formate: Ein zu importierendes Zertifikat kann in den folgenden Formaten vorliegen: DER, PEM und PKCS12

DER und PEM: bei diesen Formaten sind keine weiteren Angaben notwendig.

Liegt das Zertifikat im PKCS12-Format vor, erscheint ein Passwort-Dialog Hier müssen Sie das Importpasswort angeben. Außerdem werden Sie aufgefordert, ein neues Passwort für das Zertifikat zu vergeben. Geben Sie das Passwort zur Überprüfung noch ein zweites Mal ein.

Exportieren von Zertifikaten

Klicken Sie im Menü ‘`Zertifikat-Verwaltung`’ auf ‘`Zertifikat exportieren`’. Es gibt drei verschiedene Formate, in denen ein Zertifikat exportiert werden kann, PEM, DER und PKCS12.

Wenn Sie das Zertifikat im PEM oder DER Format abspeichern wollen, wählen Sie das zu exportierende Zertifikat aus der Liste aus und klicken im Menü ‘`Zertifikat-Verwaltung`’ auf ‘`Zertifikat exportieren`’.

Im nun erscheinenden Dateidialog wählen Sie den Speicherort aus und vergeben einen Namen für die Datei, in der das Zertifikat abgespeichert werden soll. Sie müssen außerdem noch aus der Format-Selectbox das Format auswählen: DER oder PEM. Das Zertifikat wird abgespeichert. Beim Exportieren im PEM-Format können Sie außerdem noch angeben, ob das Zertifikat alleine oder mit Schlüssel abgespeichert werden soll.

Beachten Sie, dass ein Zertifikat nur dann im PKCS12-Format exportiert werden kann, wenn ein Schlüssel zu diesem Zertifikat existiert. Verfahren Sie wie unter PEM und DER. Wählen Sie einen Namen für das Zertifikat und als Dateiformat PKCS12. Sie werden nach dem Passwort für das Zertifikat gefragt. Sie müssen ausserdem noch ein Export-Passwort eingeben. Geben Sie dieses Passwort zur Überprüfung noch ein zweites Mal ein. Dieses Passwort müssen Sie eingeben, wenn Sie das Zertifikat importieren wollen.

4.3.13 Konfiguration eines Zeitservers mit xntpd (NTP-Modul)

Mit diesem FAS Modul können Sie den Zeitserver xntpd konfigurieren. xntpd sorgt dafür, dass die Rechnerzeit mit einer externen Zeitquelle (ein Rechner mit der genauen Uhrzeit) synchron gehalten wird. Das ist wichtig, damit die Zeitstempel in den Logdateien mit Zeitstempeln anderer Logdateien (auf anderen Rechnern) vergleichbar werden.

Sie können bis zu drei Zeitserver angeben, von denen versucht wird, sich die aktuelle Zeit zu holen (Abb. 4.38 auf der nächsten Seite).

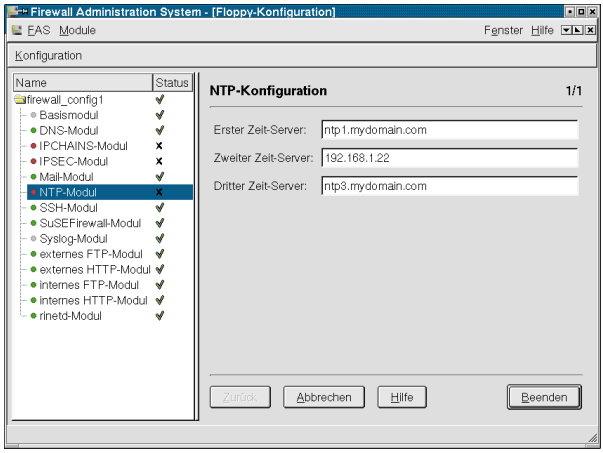


Abbildung 4.38: Zeitserver angeben im NTP-Modul

Das ntp-Protokoll ist UDP-basiert. Sie müssen die entsprechenden Ports natürlich in Ihrem Paketfilter freischalten.

Sie können die Namen oder die IP-Adressen der Zeitserver angeben.

4.3.14 Rinetd

Bei dem Programm rinetd handelt es sich um einen generischen Proxy; d. h. es handelt sich um eine Software, die auf einem Interface eine Verbindung annimmt und auf einem zweiten Interface die ankommenden Daten an einen anderen Rechner weitergibt. Dies geschieht port-abhängig. Es handelt sich sozusagen um Routing von tcp-Verbindungen auf der Application Ebene.

Rinetd kann nur 1:1 Verbindungen routen. So ist ein Einsatz als Ftp-Proxy nicht möglich, da eine ftp-Verbindung aus zwei „Kanälen“ besteht.

Die Konfiguration des rinetd erfolgt durch das rinetd-Modul des Firewall Administation Systems FAS.

Der generische Proxy rinetd sollte dann zum Einsatz kommen, wenn es kein dediziertes Application-Level-Gateway gibt (wie z. B. ftp-proxy-suite, squid usw.). Mit rinetd lassen sich so auf einfache und sichere Weise Verbindungen für z. B. pop3 durch die Firewall leiten.

rinetd unterstützt auch vollständiges Logging, d. h. alle eingehenden Verbindungen werden vom syslogd mitgeschrieben.

Lesen sie dazu auch die Manual-Seiten zu rinetd (Manual-Page von **`rinetd`** (**`man rinetd`**)).

rinetd-Konfiguration

Die Konfiguration des Programms rinetd erfolgt mit FAS. Sie können rinetd-Verbindungen einrichten, bearbeiten und löschen.

Sie benötigen folgende Daten:

- Die IP-Adresse, auf der die Firewall Verbindungen für rinetd entgegennehmen soll.
- Die Portnummer oder den Service-Namen (siehe auch `/etc/services`), auf dem die Anfragen ankommen.
- Die IP-Adresse des Hostes, der über die rinetd-Verbindung erreicht werden soll und der Port, auf den dieser Service hört.

Sie müssen natürlich auch alle Service-Ports auf den Netzwerkinterfaces, die Sie mit rinetd weiterleiten wollen, in den IP-Paketfilterregeln freischalten. Das können Sie mit FAS im SuSEFirewall-Modul durchführen.

Für die Konfiguration von TCP-Verbindungen mit rinetd stellt Ihnen das FAS das ‘`rinetd-Modul`’ zur Verfügung. In dem Modul-Fenster sehen Sie alle bereits eingerichteten rinetd-Verbindungen (Abb. 4.39).

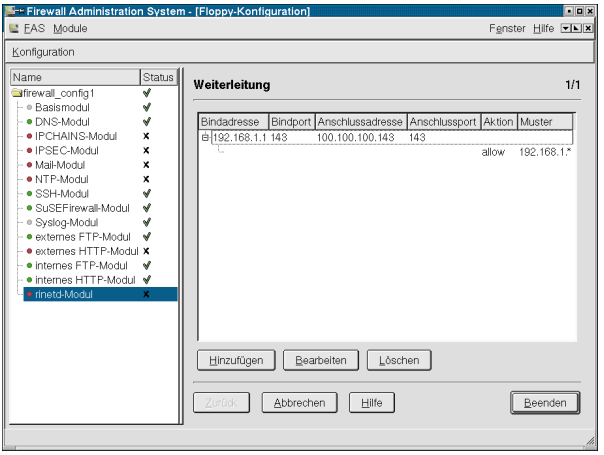


Abbildung 4.39: Rinetd-Modul mit eingerichteten rinetd-Verbindungen

Durch Doppelklicken einer bereits eingerichteten Verbindung können Sie die zusätzlichen allow- bzw. deny-Attribute sichtbar machen.

Mit den folgenden Dialogen können Sie den generischen Proxy rinetd konfigurieren. Nach dem Starten des rinetd-Moduls sehen Sie alle bisher angelegten Forwarding rules (Abb. 4.39).

Zum Anlegen einer neuen Verbindung klicken Sie auf den Button ‘`Hinzufügen`’. Es erscheint das Konfigurationsfenster des Moduls (Abb. 4.40 auf der nächsten Seite).

Eine Regel besteht aus folgenden Teilen: Bindadresse, Bindport, Verbindungsadresse, Anschlussport

Bindadresse ist die IP-Adresse, für die der rinetd eine Verbindung annehmen soll.

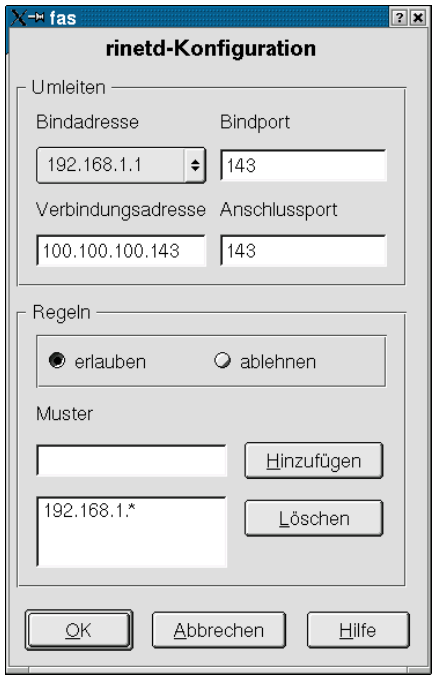


Abbildung 4.40: Rinetd-Konfigurationsfenster

Bindport ist die Portnummer des Dienstes, der weitergeleitet werden soll.

Verbindungsadresse ist die IP-Adresse des Rechners, der einen Dienst zur Verfügung stellt.

Anschlussport ist die zum Dienst zugehörige Portnummer.

Beispiel:

Sie wollen vom internen Netz auf einen pop3-Server im Internet zugreifen. Die Bindadresse ist damit das interne Interface Ihrer Firewall (z. B. 10.10.10.1). Der Bindport ist der pop3-Port (110).

Die Verbindungsadresse ist die IP-Adresse des pop3-Servers im Internet (z. B. 195.23.82.20) und der Anschlussport der Port, auf dem der pop3-Service angeboten wird (normalerweise Port 110). Ihre Eingaben müssen also folgendermaßen lauten:

```
Bindadresse     Bindport     Verbindungsadresse     Anschlussport
10.10.10.1      110          195.23.82.20           110
```

Zusätzliche Möglichkeiten:

Es ist möglich, einer Forwarding-Regel zusätzlich noch entweder Allow- oder Deny-Regeln mitzugeben. Es können nur entweder Allow- oder Deny-Regeln

einer Forwarding-Regel mitgegeben werden.

Zu Allow und Deny wird als Parameter eine IP-Adresse oder ein IP-Adressbereich angegeben. Es sind alle Ziffern (0-9), der Punkt (.), das Fragezeichen (?) und der Stern (*). Das Fragezeichen steht für jedes beliebige einzelne Zeichen, der Stern für beliebig viele Zeichen, inclusive der Null. Als Parameter sind nur IP-Adressen erlaubt.

Allow: Wenn eine Verbindung ankommt, die keiner der Allow-Regeln entspricht, wird sie sofort zurückgewiesen.

Deny: Wenn eine Verbindung von einer IP-Adresse oder einem Adressbereich kommt, der unter eine Deny-Regel fällt, wird die Verbindung sofort zurückgewiesen.

Um die Einstellungen abzuspeichern, bestätigen Sie Ihre Eingaben mit ‘OK’. Die Logausgaben werden auf den syslog der Firewall geschrieben.

Um eine bestehende Regel zu editieren, wählen Sie die entsprechende Regel in der Liste aus und klicken auf den ‘Bearbeiten’-Button. Es erscheint ein Dialog, in dem die bisherigen Einstellungen sichtbar sind. Machen Sie Ihre Änderungen und bestätigen Sie die Änderungen mit ‘OK’.

Das Löschen einer Regel erfolgt durch Auswählen einer Regel und Drücken des ‘Löschen’-Buttons.

4.3.15 VPN Connections (IPSEC-Modul)

Einführung

Das VPN Connection-Modul ermöglicht es, VP Netzwerke einzurichten. Diese Virtual Private Networks kann man sich als Tunnel zwischen zwei Hosts vorstellen, der durch das „normale“ Internet verläuft. Dieser Tunnel weiß nichts über die in ihm übertragenen Informationen.

Die VPNetzwerke werden auf der „SuSE Firewall on CD“ mit IPsec realisiert. IPsec ist eine Protokollfamilie, die es ermöglicht, sichere Verbindungen zwischen Computern herzustellen. Die Authentifizierung erfolgt durch Zertifikate. Als weitere Möglichkeit für die Authentifizierung gibt es noch die Methode des „Pre Shared Key“.

Die Daten, die durch diesen Tunnel geleitet werden, werden automatisch verschlüsselt. Die für die Authentifizierung notwendigen Zertifikate werden mit dem Keyring-Modul von FAS erzeugt bzw. importiert (vgl. 4.3.12 auf Seite 61).

Zu beachten ist Folgendes:

Um IPsec verwenden zu können, muss der IP-Paketfilter auf der „SuSE Linux Firewall on CD“ angepasst werden. Dies geschieht automatisch, wenn Sie den Paketfilter mit dem SuSE Firewall Modul in FAS erstellt haben.

Wenn Sie ein eigenes Firewall-Skript mit FAS importiert haben, müssen Sie folgendermaßen vorgehen:

In Ihrem Firewall-Skript muss eine Chain angelegt werden, die „ipsec“ heisst. Das geschieht mit dem folgenden Kommando:

```
erde: # ipchains -N ipsec
erde: # icphains -A input -j ipsec
```

Diese Regel führt dazu, dass alle ankommenden Pakete durch diesen Filter geschickt werden.

Dies sollte relativ früh in Ihrem ipchains-Filter passieren, damit alle Pakete durch die ipsec-chain laufen. Wenn das Paket nicht für die VPN-Verbindung bestimmt war, läuft es durch die anderen Filterregeln.

Die Regeln in der ipsec-chain werden vom Skript `/etc/ipsec.d/updown` gesetzt, das ausgeführt wird, wenn eine IPsec-Verbindung aufgebaut oder abgebaut wird.

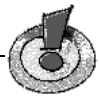
Speichern Sie wie gewohnt Ihre Filterregeln mit ipchains-save ab. Die zusätzliche Filterchain wird benötigt, damit beim Starten von IPsec die notwendigen Ports freigeschaltet werden und das Masquerading für die Pakete, die durch den Tunnel geleitet werden, abgeschaltet wird.

Die IP-Pakete, die durch den VPN Tunnel geleitet werden, werden nur in der ipchains chain „ipsec“ gefiltert. Wenn Sie die Zugriffe der VPN-Partner auf bestimmte Dienste beschränken wollen, müssen Sie weitere Regeln in der Chain „ipsec“ hinzufügen. Diese Regeln können Sie mit FAS im Dialog „IP Filter Regeln für VPN Tunnel“ (s. 4.3.15 auf Seite 74) erzeugen. Hierbei ist zu beachten, dass diese Regeln dann für alle VPN-Verbindungen dieser Firewall-Konfiguration gelten.

Einrichten von Ipsec-Tunneln mit FAS

Im ersten Dialog des Moduls (‘`Wählen Sie das lokale Zertifikat`’) werden Sie aufgefordert, ein X.509-Zertifikat für die Authentifizierung auszuwählen (Abb. 4.41 auf der nächsten Seite). Dieses Zertifikat wird auf dem Firewall-Rechner verwendet, dessen Konfiguraton gerade bearbeitet wird. Zur Erstellung von Zertifikaten siehe Kap. 4.3.12 auf Seite 61.

Wenn Sie keine starke Authentifizierung einsetzen wollen, können Sie auch auf ein Zertifikat verzichten.



Hinweis

Unter „starker Authentifizierung“ versteht man eine Authentifizierung durch Schlüssel und Passphrase, also durch zwei Kriterien.

Im zweiten Dialog richten Sie die einzelnen VPN-Verbindungen ein. In einer Tabelle werden Ihnen alle bisher eingerichteten VPNs angezeigt (Abb. 4.42 auf Seite 73).

Wählen Sie ‘`Hinzufügen`’, um eine neue VPN-Verbindung einzurichten. In dem erscheinenden Dialog sehen Sie zwei Kartei-Karten (s. Abb. 4.43 auf Seite 74: ‘`Allgemeine Einstellungen`’ und ‘`VPN Verbindung`’

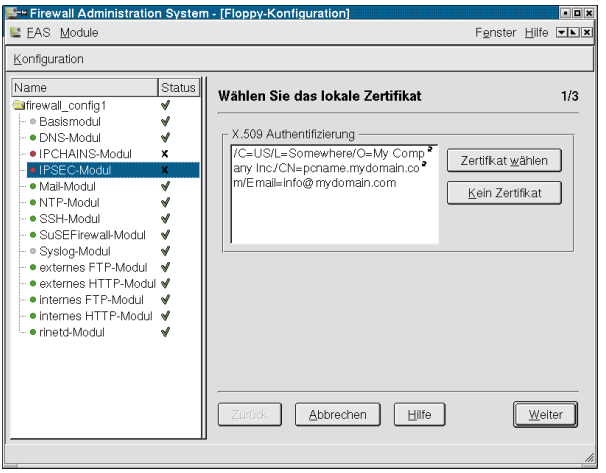


Abbildung 4.41: Lokales Zertifikat wählen

Allgemeine Einstellungen

Sie werden aufgefordert, einen Namen für die Verbindung einzugeben. Dies erleichtert Ihnen die Zuordnung der Verbindung, falls Sie mehrere Tunnel einrichten wollen (Sie haben z. B. mehrere Filialen an unterschiedlichen Standorten, die Sie über VPNs verbinden wollen). Der Name einer Verbindung darf nur Buchstaben, Zahlen, Unterstriche und Bindestriche enthalten.

Sie können bestimmen, ob die „SuSE Firewall on CD“ auf ankommende VPN-Verbindungen warten soll (Server Mode) oder ob die Firewall beim Booten schon eine Verbindung zu einem anderen VPN-Server öffnen soll (Client-Modus) (z. B. Außenstellen, die eine Verbindung zur Hauptfiliale haben sollen, werden den Client-Modus wählen, die Hauptfiliale den Server-Modus).

Desweiteren legen Sie den Authentifizierungs-Mechanismus für diese Verbindung fest. Sie können X.509-Zertifikate verwenden (empfohlen) oder einen „Pre Shared Key“. Das X.509-Zertifikat ist vergleichbar mit einem Personalausweis, den Sie für Ihren Rechner ausstellen. Mit diesem Zertifikat authentifiziert sich der Rechner an allen VPN-Gegenstellen. Das ist auch der Grund dafür, dass Sie pro Rechner nur ein Zertifikat auswählen können.

Der „Pre Shared Key“ ist eine beliebige Zeichenfolge. Zu beachten ist, dass keine Anführungszeichen (double quote) im shared-key vorkommen dürfen. Jede Verbindung kann natürlich einen eigenen „Pre Shared Key“ haben, aber der „Pre Shared Key“ muss natürlich an beiden Enden eines Tunnels gleich sein. Die Übermittlung des „Pre Shared Keys“ muss auf eine sichere Weise bewerkstelligt werden, da sich jeder, der diesen Key kennt, am VPN-Gateway authentifizieren kann und Zugang erhält. Deshalb ist die Verwendung von X.509-Zertifikaten auf jeden Fall vorzuziehen.

Um die Konfiguration zu vervollständigen, wählen Sie nun den Reiter ‘`VPN-Verbindung`’ aus (Abb. 4.44 auf Seite 75).

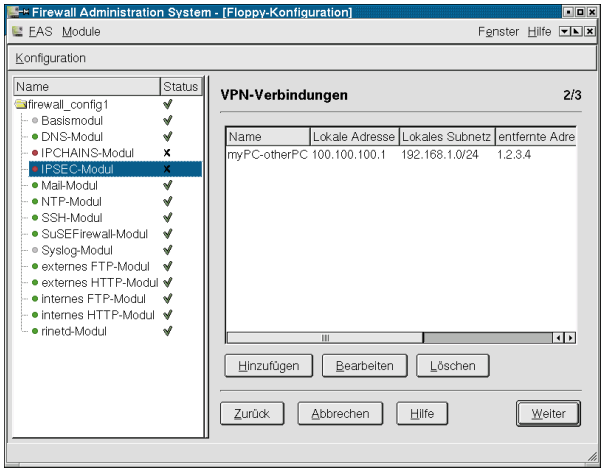


Abbildung 4.42: Eingerichtete VPN-Verbindungen

Lokale Konfiguration

Geben Sie unter ‘`IP-Adresse`’ die IP-Adresse Ihrer Firewall an, auf der VPN-Verbindungen angenommen werden sollen. In das Feld ‘`Subnetz`’ tragen Sie das IP-Netzwerk ein, das von einer ankommenden VPN-Verbindung aus erreicht werden soll. Zu beachten ist bei ‘`Subnetz`’, dass das Netz aus einem anderen IP-Adressenbereich sein muss als auf der Remote-Seite (vgl. Abb. 4.44 auf Seite 75. Auf der anderen Seite des Tunnels (also der Remote-Seite) wird automatisch eine Route in dieses Subnetz gesetzt.

Das Feld Gateway müssen Sie ausfüllen, wenn das andere VPN-Gateway nur durch diesen Router erreichbar ist.

Entfernte Konfiguration

Hier gibt es zwei Möglichkeiten: Die „Road Warrior“-Konfiguration oder die „feste IP-Adresse“.

Die Road Warrior-Konfiguration ermöglicht es einem Client, von einer beliebigen IP-Adresse aus eine Verbindung zum VPN-Server aufzubauen (z. B. Einwahl ins Internet bei einem beliebigen Provider, Bereitstellen des Zugangs zum Firmennetz). Das Feld ‘`Subnetz`’ ist bei Road Warrior-Konfiguration deaktiviert.

‘`Feste IP-Adresse`’ setzt voraus, dass der Client den Zugang zum Internet durch eine feste IP-Adresse bewerkstelligt.

Das Feld ‘`Subnetz`’ bezeichnet das Netzwerk, dass hinter dem Client liegt und von der anderen Seite des Tunnels erreicht werden soll. Beachten Sie, dass das Subnetz aus einem anderen IP-Adressbereich stammen muss als auf der Local-Seite. Bei Aufbau des Tunnels wird automatisch eine Route in dieses Subnetz gesetzt.

‘`Gateway`’ gibt, falls notwendig, den Router an, über den das andere VPN-Gateway erreicht werden kann.

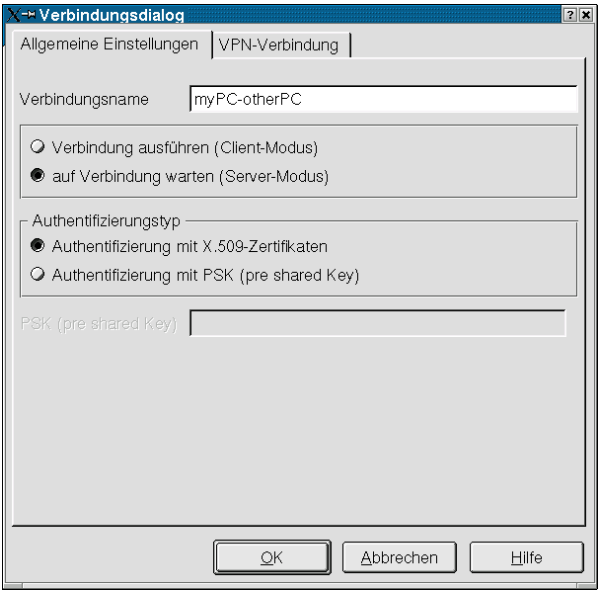


Abbildung 4.43: VPN-Verbindungsdialog - Allgemeine Einstellungen

Falls Sie für das Authentizierungs-Verfahren-Zertifikate verwenden, müssen Sie ein (vorher mit dem Keyring-Modul erstelltes oder in den Keyring importiertes) Zertifikat angeben (s. 4.3.12 auf Seite 61). Mit ‘`Auswählen`’ können Sie aus der Liste der erstellten Zertifikate eines auswählen. Es erscheint ein Dialog mit einer Liste der verfügbaren Zertifikate (Abb. 4.45 auf Seite 76).

ipchains Regelsatz für VPN Tunnel

In diesem Dialog können Sie die Dienste freischalten, die durch den VPN-Tunnel erreichbar sein sollen (Abb. 4.46 auf Seite 77).

Lokaler Rechner zu entferntem Rechner: Hier werden die Dienste freigeschaltet, die durch den Tunnel auf der entfernten Site erreicht werden sollen. Wählen Sie die freizuschaltenden TCP/UDP-Ports/Services aus den angezeigten Listen durch Anklicken aus.

Entfernter Rechner zu lokalem Rechner: Hier werden die Dienste freigeschaltet, die durch den Tunnel auf der lokalen Site erreicht werden sollen. Wählen Sie durch Anklicken die Ports/Services aus, die freigeschaltet werden sollen.

Falls Sie eine geänderte Auswahl haben wollen, weil ein Service nicht in der Liste steht, editieren Sie eine der beiden folgenden Dateien mit einem Editor Ihrer Wahl:

```
/etc/fas/IpsecTCPServices.conf
/etc/fas/IpsecUDPServices.conf
```

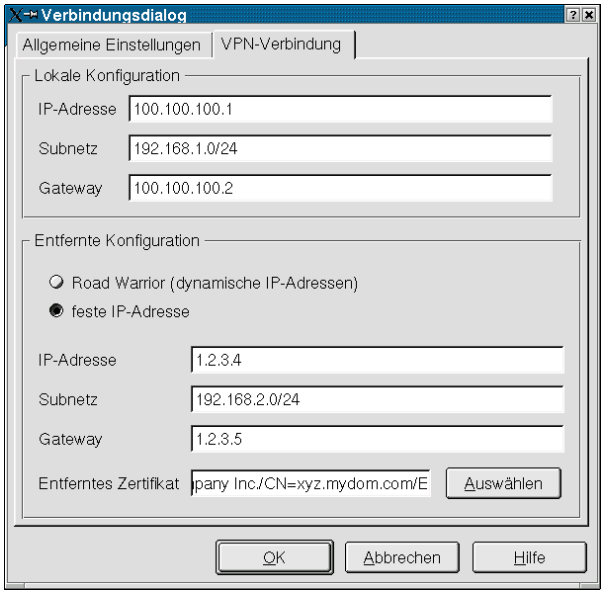


Abbildung 4.44: VPN-Verbindungsdialog - lokale und entfernte Konfiguration

und fügen die gewünschten Ports/Services hinzu. Sie haben auch die Möglichkeit, den Netzwerkverkehr durch den Tunnel jeweils komplett freizugeben. Aktivieren Sie dazu jeweils die Checkbox '`Alles vom ... erlauben`'.

Diese Regeln gelten natürlich nur für die VPN-Verbindungen. Alle anderen von Ihnen getroffenen Einschränkungen bleiben unberührt.

Verteilung der Zertifikate

Um die Zertifikate für eine VPN-Verbindung auf die Clients zu verteilen, wählen Sie im Fenster '`VPN-Verbindungen`' die Verbindung aus, deren Zertifikate Sie exportieren wollen. Klicken Sie mit der rechten Maustaste auf die ausgewählte Verbindung und wählen Sie '`Zertifikate exportieren`' an.

Sie müssen dazu zuerst das Zertifikat-Passwort eingeben und dann zweimal ein Export-Passwort dafür. Es erscheint ein Verzeichnis-Listing, in dem Sie den Speicherort auswählen können. Die Daten werden an diesen Ort geschrieben. (Bei Windows-Clients sollten Sie die Daten auf eine DOS-formatierte Diskette schreiben.)

Die Zertifikate können wie folgend exportiert werden:

- Die CA im PEM-Format als `cacert.pem`
- Das Zertifikat dieser Konfiguration im PEM-Format als `srvCert.pem`
- Das Zertifikat und der Key des mit diesen Zertifikaten zu konfigurierenden Rechners im PKCS12 Format als `remCert.p12` Hierfür müssen Zertifikat und Schlüssel im Keyring gespeichert sein.

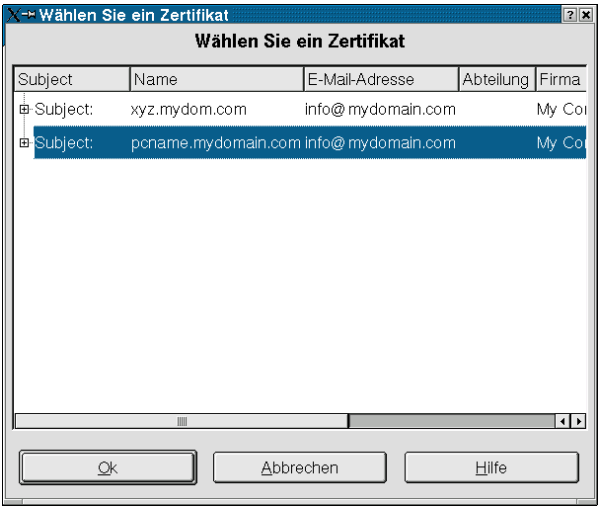


Abbildung 4.45: Entferntes Zertifikat auswählen

Testen des Tunnels

- Verbinden der Clients mit dem Server
- Linux - Linux
- Linux - andere VPN-Gateways
- Einrichten von Windows Clients

4.3.16 Abspeichern der Konfiguration

Eine Konfiguration können Sie speichern, indem Sie im Menü '`Konfiguration`' auf den Menüpunkt '`Konfiguration speichern`' klicken. Wenn Sie die Konfiguration verlassen und Änderungen vorgenommen haben, werden Sie gefragt, ob Sie diese speichern wollen. Die Konfiguration wird mit **`tar`** archiviert und mit **`gzip`** komprimiert und auf der Festplatte unter

`/var/lib/fas/<username>/configs/<konfigurationsname>.tar.gz`

abgelegt. Kein normaler Benutzer auf dem Adminhost kann diese Konfigurationen lesen. Nur '`root`' hat dazu die nötigen Rechte.

Um eine Diskette zu erstellen, legen Sie eine in das Laufwerk, wählen Sie die zu speicherende Konfiguration aus und klicken dann im Menü erst auf '`Konfiguration`' und dann auf '`Diskette schreiben`'. Jetzt wird die Diskette geschrieben. Zuvor muss die Konfiguration als „richtig konfiguriert" erkannt werden, was mit einem grünen Haken im linken Bereich des Dialogs gekennzeichnet wird.

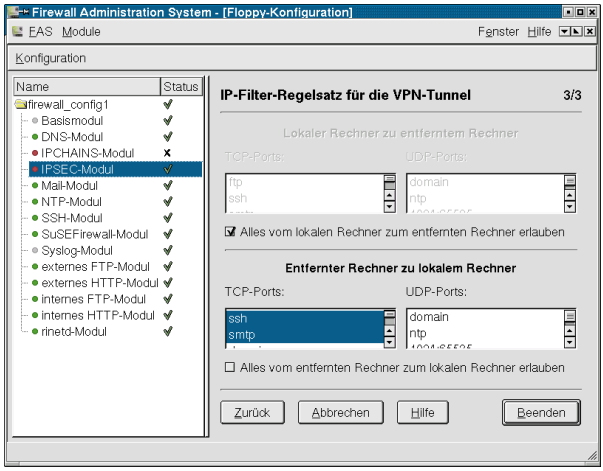


Abbildung 4.46: Regelsatz für VPN-Tunnel

4.4 Bearbeiten einer bestehenden Firewall-Konfiguration

Um eine bestehende Firewall-Konfiguration zu bearbeiten, starten Sie das FAS. Melden Sie sich über das Menü ‘FAS’ → ‘Anmelden’ als der Benutzer an, als der Sie die Konfiguration erstellt haben, und geben Sie Ihr Passwort ein. Jetzt erhalten Sie eine Liste der bisher von diesem Benutzer erstellten Konfigurationen.

Wählen Sie aus der Liste die Konfiguration aus, die Sie bearbeiten wollen. Ein Doppelklick auf den Konfigurationsnamen in der Liste im linken Fenster lässt Sie in dem entsprechenden Modul einen der Dienste bearbeiten.

4.5 Testen der Konfiguration

Die mit dem Administrations-Programm erstellte Konfiguration muss vor dem produktiven Einsatz noch getestet werden.

Dazu wird die Firewall noch ohne Verbindung zum Internet/Intranet gestartet. Um die Tests durchzuführen, verbindet man die Firewall direkt (Crossover-Kabel) mit dem Adminhost.

Tests für den Paketfilter kann man einfach mit einem Portscanner durchführen. Hierfür ist auf dem Adminhost das Programm nmap installiert. Wenn Sie den Portscan vom Adminhost aus durchführen, beachten Sie, dass Sie den Paketfilter des Adminhosts abschalten müssen. Melden Sie sich als Benutzer ‘root’ an und geben folgendes Kommando auf einer Konsole ein:

```
root@adminhost: # SuSEfirewall stop
```

So wird sichergestellt, dass alle zurückkommenden IP-Pakete vom Adminhost angenommen werden können. Vergessen Sie nicht, den Paketfilter nach Abschluss des Tests wieder zu aktivieren:

```
root@adminhost: # SuSEfirewall start
```

Nach dem Portscan sollten das Scan-Ergebnis und das Logfile auf der Firewall dokumentiert und aufbewahrt werden.

Prüfen Sie die Funktion der folgenden Dienste:

- Testen Sie den Nameserver, z. B. mit **`nslookup`** plus Name der Firewall. Kontrollieren Sie das Logfile, z. B. mit **`grep named /var/log/messages`**. Es dürfen keine Meldungen, die „error“ enthalten, vorkommen.
- Testen Sie die Mailrelays, indem Sie eine E-Mail verschicken und die Log-Dateien `/var/log/mail` und `/var/log/messages` kontrollieren. Suchen Sie in den logfiles nach „postfix“ (**`grep postfix /var/log/mail`**)
- Testen Sie die FTP-Proxies, z. B. mit **`telnet`** auf Ihre Firewall.
- Testen Sie den HTTP-Proxy, indem Sie versuchen, von einem Client aus das Internet zu erreichen.
- Testen Sie `ssh`, indem Sie sich von einem Client aus auf der Firewall anmelden.

Überprüfen Sie immer alle Vorgänge anhand der Logfiles.

4.6 Dokumentation der Konfiguration, der Tests und der Ergebnisse

Es ist sehr wichtig, dass Sie die Konfiguration, die durchgeführten Tests und deren Ergebnisse dokumentieren. Halten Sie also fest, was durch die Konfiguration erlaubt oder verboten ist und wie beides gewährleistet wird.

Anhand solcher Dokumentation können Sie eventuelle Konfigurationsfehler auffinden und beheben. Die Dokumentation ist auch für eine Auditierung der Firewall notwendig.

4.7 Überwachung der Firewall

Wie bereits mehrfach betont, ist eine Firewall ohne ständige Überwachung nur sehr eingeschränkt wirksam. Für die Überwachung der Firewall stehen auf dem Adminhost der Firewall einige Werkzeuge bereit. Die wichtigste Quelle für Informationen sind die Log-Dateien, die von der Firewall je nach Konfiguration auf Festplatte oder Loghost geschrieben werden.

Als Werkzeuge zur Auswertung der Logfiles stehen folgende Programme zur Verfügung:

- xlogmaster
- logsurfer

- sylog-ng

Folgende Netzwerk- oder Paketsniffer können Sie zur Überwachung Ihrer Firewall einsetzen:

- ntop
- tcpdump
- ethereal

Mit folgenden Portscannern ist es möglich, die Firewall auf offene Ports hin zu untersuchen und die Paketfilter-Konfiguration zu überprüfen:

- nmap
- nessus

Darüber hinaus können Sie natürlich auch selbstgeschriebene Shell- oder Perlskripte verwenden.

4.8 Konfiguration von syslog-ng

Um den Loggin Daemon **`syslog-ng(8)`** auf dem Loghost zu konfigurieren melden Sie sich als Benutzer `'root'` auf einer Konsole an oder geben das Kommanado **`su - root`** in einem xterm ein. Falls der SuSE Linux Adminhost for Firewall nicht Ihr Loghost sein sollte, dann kopieren Sie das Programm `/opt/fas/sbin/fas_syslogng_config.pl` auf Ihren Loghost.

Starten Sie das Programm als `'root'` mit folgendem Befehl:

```
root@loghost: # /opt/fas/sbin/fas_syslogng_config.pl
```

Geben Sie den Hostnamen Ihrer Firewall an. Legen Sie fest, ob syslog-ng beim Systemstart gestartet wird. Default ist "yes".

Der Hostname der Firewall muss in eine IP-Adresse aufgelöst werden können. Das können Sie durch einen Eintrag in die Datei `/etc/hosts` auf Ihrem Loghost sicherstellen. Vergleichen Sie dazu das Beispiel 4.8

```
# Eintrag für Firewall-Logging
# ip-address of firewall   hostname.mydomain.com hostname
# z. B.
192.168.0.1    stargate.mydomain.com  stargate
```

Datei 4.8.1: Beispieleintrag für die Datei /etc/hosts

5 SuSE Linux Live-CD for Firewall

5.1 Einführung

Die „Live-CD“ zur SuSE Linux Firewall on CD ist der „ausführende“ Teil der Firewall. Die Live-CD ist ein minimales, nach Sicherheitskriterien ausgerichtetes SuSE Linux. Das betrifft die Programme, die zur Verfügung stehen, ebenso wie den Kernel selbst. Die „SuSE Firewall on CD“ ist darüber hinaus ein „Application Level Gateway“, das heißt, es sollte aus Sicherheitsgründen kein Routing von IP-Paketen vorgenommen werden. Die Weiterleitung von Anfragen an Dienste wird durch Applikationen (= Proxies) gehandhabt.

Mit Proxies und Non-Forwarding von IP-Paketen alleine kann man noch nicht verhindern, dass (unerwünschte) IP-Pakete vom Internet ins Intranet und umgekehrt gelangen können. Diese Firewall-Funktionalität wird durch den Paketfilter des Kernels übernommen, der mit ipchains(8) konfiguriert wird. Verwendung findet hier das Konzept der Live-CD. Das bedeutet, dass sich das Betriebssystem und alle Programme auf einem Read-Only-Filesystem auf einer CD befinden. Beim Booten wird eine RAM-Disk erzeugt, in welche die Live-CD gemountet wird. Eine Wiederherstellung des „status quo ante“ ist durch einfaches Rebooten des Rechners möglich. Auch das Update der „SuSE Linux Firewall on CD“ ist dadurch sehr einfach: Tauschen Sie einfach die Live-CD gegen die aktuelle Update-CD aus und starten Sie Ihren Firewall-Rechner neu.

Die Konfiguration des Systems und der Dienste erfolgt durch eine Diskette, auf der alle notwendigen Konfigurationsdateien abgespeichert sind. Diese wird beim Boot-Vorgang „read only“ gemountet, vorsichtshalber sollte sie dennoch auch schreibgeschützt werden. Die Daten der Konfigurationsdiskette werden in die RAM-Disk kopiert, danach wird der Datenträger wieder aus dem Dateisystem entfernt.

Hardwareanforderungen:

- Die „SuSE Linux Live-CD for Firewall“ ist auf jedem **`ix86`**, ab x=5, lauffähig. Empfohlen wird mindestens ein **`Pentium II`**.
- Es sind mindestens `128 MB` RAM notwendig,
- ein Diskettenlaufwerk 3,5 Zoll,
- ein bootfähiges CD-ROM-Laufwerk und
- mindestens zwei Netzwerkinterfaces.

Dieses Kapitel liefert keine Anleitung zur Konfiguration der Dienste auf der Firewall, sondern eine technische Dokumentation für den versierten Administrator,

der sich mit den Interna des Systems auseinander setzen will. Hier werden auch Details der Konfigurationsdateien der Dienste auf der Live-CD beschrieben. Zur Konfiguration sollte das Firewall Administration System (FAS) auf dem SuSE Firewall Administration Host verwendet werden.

5.2 Beschreibung der SuSE Linux Live-CD for Firewall

Die „SuSE Linux Live-CD for Firewall“ ist eine Live-File-System-CD, von der alle Programme direkt laufen. Theoretisch ist es möglich, den Firewall-Rechner ohne Festplatte zu betreiben. Sie sollten allerdings beachten, dass für Proxy-Dienste wie z. B. Squid oder postfix eine Festplatte für das Cache- bzw. Spool-Verzeichnis notwendig ist. Eine Festplatte ist auch dann notwendig, wenn Sie die Log-Meldungen des syslogd lokal speichern wollen. Um das Firewall-System in Betrieb zu nehmen, legen Sie die CD und die mit dem SuSE Firewall Adminhost erstellte Konfigurationsdiskette ein und booten den Rechner.

5.3 Die Dienste auf der Firewall

Auf der „SuSE Linux Live-CD for Firewall“ befinden sich „Application Level Gateways“ (Proxies) für die gängigsten und wichtigsten Internetprotokolle:

DNS (engl. *Domain Name System*): Die Umsetzung von IP-Adressen in „Fully Qualified Domain Names“ und umgekehrt erfolgt mit bind8

SMTP Den Transport von E-Mail übernimmt postfix

HTTP/HTTPS – das Protokoll des WWW: Squid, httpf, transproxy, tinyproxy

FTP Für die Dateiübertragung von einem Host zu einem anderen wird ftp-proxy-suite benutzt.

SSH Der „remote login“ mit verschlüsselter Übertragung erfolgt mit openssh, die Authentisierung mit RSA-Schlüssel-Paaren.

rinetd Generischer tcp Proxy rinetd

ntp Zeitserver xntpd

ipsec FreeS/WAN

Bei all diesen Programmen handelt es sich um Open-Source-Software. Auf der „SuSE Linux Live-CD for Firewall“ laufen alle diese Prozesse in chroot-Umgebungen.

Um die Sicherheit des Systems noch weiter zu erhöhen, werden folgende Programme bzw. Kernelmodule für den auf der Live-CD eingesetzten Linux Kernel (2.2.19) verwendet: `secumod`, `compartment`, `OpenWall-Patches`.

5.3.1 IPCHAINS

Der Paketfilter des Linux-Kernels 2.2.xx wird mit dem Programm ipchains konfiguriert. Mit ipchains ist eine äußerst flexible Konfiguration des Kernel-Paketfilters möglich. Lesen Sie auch hierzu die Man-Page von ipchains(8).

Standardmäßig kennt ipchains(8) drei Paketfilter-„Chains“: input-chain, forward-chain und output-chain.

Diese drei entscheiden über das Schicksal eines IP-Paketes, das auf einem Interface ankommt. Es ist empfehlenswert, für diese „chains“ eine Policy festzulegen, die alle Pakete ablehnt. Dies ist dann das Default-Verhalten der chain: Alles, was nicht ausdrücklich erlaubt ist, ist verboten.

IP-Pakete durchlaufen die Chains und werden nach Ursprungs- und Ziel-Adresse sowie -Port entsprechend behandelt, das heißt weitergeleitet, verworfen oder zurückgewiesen. Auf der „SuSE Linux Live-CD for Firewall“ gibt es grundsätzlich zwei Möglichkeiten, ipchains-Filterregeln zu konfigurieren. Die erste und wohl bequemere Möglichkeit ist die Verwendung des SuSE Firewall Skripts. Die Konfiguration für das SuSE Firewall Skript erfolgt in Abhängigkeit von den konfigurierten und aktivierten Diensten. Der SuSE Firewall Adminhost bietet mit seinem Firewall Administration System (FAS) einen bequemen Zugriff auf das SuSE Firewall Skript. Die zweite Möglichkeit besteht darin, dass Sie einen eigenen Paketfilter mit ipchains konfigurieren. Zunächst geben wir Ihnen eine Übersicht über das SuSE Firewall Skript und anschließend Hinweise zur Erstellung eines eigenen Paketfilters.

Das SuSE Firewall Skript und seine Konfiguration

Dies ist eine technische Beschreibung, wie die Filterregeln generiert werden, und welche Hintergründe das neue Design des SuSE-Firewall-Skriptes hat. Diese Dokumentation ist aber *keine* Beschreibung, wie die Firewall konfiguriert wird – die Konfigurationsdatei `/etc/rc.config.d/firewall.rc.config` enthält ausreichend Kommentare, die die Bearbeitung erleichtern. Des Weiteren finden sich in der Datei `EXAMPLES` im Verzeichnis `/usr/share/doc/packages/SuSEfirewall` einige Beispielkonfigurationen. Inzwischen gibt es auch eine FAQ-Liste im gleichen Verzeichnis. Beachten Sie bitte, dass in der Dokumentation immer von „Firewall“ die Rede sein wird, obwohl dieses Skript dies streng genommen nicht ist. Dieses Paket ist ein so genannter „Paket-Filter“, der auf TCP/IP-Ebene Daten zulässt oder verbietet. Mit anderen Worten: Wenn Sie einen WWW-Server betreiben und Sie die Kommunikation mit ihm und z. B. dem Internet erlauben, dann kann Sie dieses Skript nicht schützen, wenn der Webserver als solcher ein Sicherheitsproblem aufweist. Es ermöglicht Ihnen jedoch, Dienste zu schützen, die nicht zugänglich sein sollen, sowie Angreifer über Ihre Konfiguration im Dunkeln zu lassen und Angriffe durch das Feststellen der Filterverstöße zu erkennen.

Die Ansprüche an das Design des SuSE Firewall Skripts sind:

- **Sicherheit über alles**

  Wer dieses Paket installiert und konfiguriert, erwartet, dass das Skript alles tut, was möglich ist, um das System abzusichern. Ein Benutzer muss aber dafür in Kauf nehmen, dass einige Dinge schwieriger oder eventuell (in wenigen Fällen) überhaupt nicht über dieses Paket konfiguriert werden können. Zudem ist mit der Einrichtung einer solchen Firewall ein gewisser Zeitaufwand verbunden.

- **Bei Fehler keine Kompromittierung des Systems**

  Ein Fehler im Skript oder ein Fehler in der Konfigurationsdatei sollte nicht zu offenen Filterregeln führen. Dieses Ziel ist in bestimmten Bereichen nur schwer umzusetzen. SuSE hat sich Mühe gegeben, dieses Ziel zu erreichen.

- **Einfache Konfiguration**

  Es werden einfache Fragen gestellt – zudem werden nur so viele gestellt, als unbedingt notwendig sind. Das ist natürlich die größte Herausforderung – und trotzdem muss man Wissen zu TCP/IP, Administrator-Kenntnisse, ein Gefühl für Sicherheit und Geduld mitbringen…

- **Automatisierte Konfiguration**

  Um die Konfiguration zu vereinfachen und auch dynamische Systeme leichter zu unterstützen, hat das SuSE-Team versucht, so viele Daten wie möglich erst zum Zeitpunkt des Startens des Firewall-Skriptes in Erfahrung zu bringen.

- **Unterstützung von dynamischen IP-Adressen + Netzen**

  Es werden nicht nur dynamische IP-Adressen, sondern auch mehrere Netzwerkkarten (unbegrenzt viele) zum Internet wie zu einem internen Netz unterstützt.

Im folgenden Abschnitt wird mehrfach von Filterregeln für interne Interfaces und Netze gesprochen. Filterregeln, die sich auf interne Interfaces oder Netze beziehen, werden nur abgearbeitet, wenn diese beim Starten des Firewall-Skripts konfiguriert und vorhanden sind. Wenn diese nach dem Starten des Skripts erst zugänglich werden, z. B. weil das Interface nach innen zuerst abgeschaltet ("down") war, dann ist keine Kommunikation mit diesem Netz möglich!

Der Ablauf des SuSE-Firewall-Skripts, das sich in `/sbin` befindet, stellt sich folgendermaßen dar:

a) Zuerst wird die Konfigurationsdatei `/etc/rc.config.d/firewall.rc.config` eingelesen. Der Benutzer muss `/etc/rc.firewall` erst konfigurieren, bevor etwas passieren kann. Diese Dateien werden bei der Verwendung von FAS angelegt.

b) Dann werden die Hilfsprogramme wie sed, awk, grep, ifconfig, netstat und natürlich ipchains gesucht. Wenn eines dieser Programme nicht auffindbar ist, wird mit einer Fehlermeldung abgebrochen. Als Nächstes wird noch

die Kernel-Version kontrolliert, um festzustellen, ob sie ipchains unterstützt. Das Skript wird auch abgebrochen, wenn ein 2.0–Kernel identifiziert wird oder gibt eine Warnung aus, falls die Version des Kernels nicht identifiziert werden kann.

c) Jetzt folgt die Interpretation der Konfigurationsdatei und die Ermittlung der momentanen Daten, die wichtig sind. So werden für alle im Skript konfigurierten Netzwerkkarten die Daten wie IP-Adresse und Netzmaske ausgelesen. Ist ein Interface nicht "up" (z. B. ein ISDN- oder PPP-Interface), werden trotzdem später Filterregeln im Skriptablauf hierfür generiert, jedoch nur einige rudimentäre Schutzmechanismen. Nach dem Aufbau einer Verbindung mit z. B. ISDN sollte das SuSE-Firewall-Skript noch einmal gestartet werden.

d) Dann geht es los! Zuerst werden die Regeln zurückgesetzt und der Default für eingehende Pakete und für solche, die die Firewall routen soll, auf "verwerfen" gesetzt. Sollte also aus irgendeinem Grund für ein Paket im Skript keine Regel existieren, so wird es immer verworfen. Pakete, die die Firewall verlassen wollen, werden hier auf den Vorgabe-Wert "erlaubt" gesetzt.

e) Wenn die Firewall auf "routen" eingestellt ist, wird das Routing aktiviert.

f) Das `/proc`-System erlaubt es, auf einfachem Wege den Kernel zur Laufzeit des Systems zu konfigurieren. Das macht sich das Skript zu Nutze, um einige Sicherheitsoptionen anzuschalten. Für viele muss hierfür aber erst die Option `FW_KERNEL_SECURITY` in der Konfigurationsdatei auf "yes" gesetzt werden, da die Auswirkungen komplex sein können.

g) Dann wird – ganz wichtig – jeder Verkehr über das Interface "localhost" freigegeben.

h) Jetzt kommen die Regeln für "IP Spoofing" und für "Umgehungsverhinderung" an die Reihe. Diese Regeln sorgen dafür, dass externe und interne Attacken erkannt und abgewiesen werden, die vorgaukeln, im jeweils anderen Netzsegment zu sein. Gleichzeitig werden auch direkte Zugriffsversuche auf das interne Netz verhindert.

i) Die Redirecting-Regeln, die dann folgen, können dazu benutzt werden, Zugriffe auf das interne Netz oder lokale Ports auf einen speziellen Port der Firewall umzuleiten.

j) Wer an ein internes (vertrauenswürdiges?) Netzwerk angeschlossen ist, kann in der Konfigurationsdatei festlegen, ob die Firewall gegen Angriffe von innen geschützt werden soll oder nicht. Ist das nicht der Fall, wird an dieser Stelle jeder Verkehr vom internen Netz auf die Firewall freigegeben. Die Option hierfür lautet `FW_PROTECT_FROM_INTERNAL` .

Dann werden Regeln für ICMP, TCP und UDP generiert.

k) ICMP-Regeln werden in zwei Stufen erstellt. Zuerst werden spezielle ICMP-Pakete je nach Konfiguration erlaubt oder verboten, z. B. "ping" auf die Firewall, "Source Quench"-Meldungen des nächsten vorderen Routers sowie

Antwortpakete für ähnliche Programme wie traceroute. Die zweite Stufe bilden allgemeine Konfigurationen, die gefährliche ICMP-Pakete verbieten und wichtige erlauben. Das interne Netz darf die Firewall immer mit "ping" erreichen.

l) Bei den TCP-Regeln werden zuerst die konfigurierten Dienste nach außen freigegeben, anschließend die für vertrauenswürdige Netze und letztendlich die für das interne Netz. Im Anschluss wird der Port 113 so konfiguriert, dass er einen Verbindungsreset sendet, um unnötige Wartezeiten (z. B. beim Senden von E-Mails) zu verhindern. Nun kommt ein besonderer Automatismus zum Zug: Wer `FW_AUTOPROTECT_GLOBAL_SERVICES` auf "yes" gesetzt hat, dessen Dienste werden durch Filterregeln geschützt, die *nicht* auf ein spezielles Interface hören (also auf `0.0.0.0` oder `INADDR_ANY`). Dadurch kann man gegebenenfalls alle hohen Ports für eingehende Verbindungen freigeben, weiß aber trotzdem seine Datenbanken etc. geschützt, die beispielsweise auf Port `4545` laufen. Zum Abschluss werden die Regeln generiert, ob oder wie auf unprivilegierte Ports (zwischen `1024` und `65535`) zugegriffen werden darf: gar nicht; nur in `/etc/resolv.conf` definierte Nameserver; nur Verbindungen, die von einem bestimmten Ursprungsport kommen (nicht empfehlenswert, dieser Schutz ist leicht zu umgehen); alle Verbindungen. Interne Systeme dürfen *immer* auf die unprivilegierten Ports zugreifen – das AUTOPROTECT schützt hier aber Dienste.

m) Das Gleiche wird für UDP vorgenommen, nur ist hier ein Verbindungsreset für Port `113` nicht notwendig.

n) Anschließend kommen die Routing-Regeln an die Reihe, die definieren, auf welche Systeme von außen auf ein internes Netz zugegriffen werden darf. Das sollte aus nahe liegenden Gründen natürlich nicht benutzt werden!

o) Jetzt erfolgt erst die Konfiguration der Regeln für Masquerading.

p) Sehr wichtig ist die Konfiguration von zusätzlichen Logmechanismen für besondere Pakete, z. B. verbotene TCP-Pakete, die eine Verbindung aufbauen wollen etc. Wenn `LOG_*_ALL` gesetzt wird, wird wirklich *jedes* Paket geloggt, was viele Logeinträge erzeugt, und deshalb nur zur Fehlerermittlung benutzt werden sollte.

q) Zu allerletzt kommen ein paar Optimierungsregeln für SSH, FTP, WWW, Syslog und SNMP, um diese schneller oder sicherer (hinsichtlich der Übertragung im Netz) zu machen.

Damit endet das Skript. Im Fehlerfall ist der Rückgabewert 1, wenn alles in Ordnung war, ist der Rückgabewert 0.

Wichtig ist nun noch das Initialisieren der Firewall während des Bootens. Das eigentliche rc-Skript heißt `/sbin/init.d/firewall`. Es wird in dem Runlevel 2 mit `S04firewall_init` und `S99firewall_setup` aufgerufen. `S04` erzeugt nur rudimentäre Regeln und gibt keinerlei Fehler aus. Dies macht erst der `S99`-Durchlauf des Skriptes, wenn alle Dienste und Interfaces vollständig konfiguriert sind. K51firewall entfernt beim Herunterfahren ("Shutdown") alle Filterregeln und erlaubt jegliches Paket, schaltet aber das Routing ab.

Dynamisch aus Dialup-Skripten sollte die Firewall immer als

`/sbin/init.d/rc2.d/S99firewall_setup start`

aufgerufen werden, damit nur dann Filterregeln generiert werden, wenn das auch so konfiguriert wurde.

TRACEROUTE

Wer möchte, dass traceroute und ähnliche Programme funktionieren, muss folgendes konfigurieren:

```
FW_ALLOW_FW_TRACEROUTE=yes  (ganz am Ende in der Experten-Konfig)
FW_ALLOW_FW_PING=yes
FW_ALLOW_INCOMING_HIGHPORTS_UDP=yes
```

Wenn Sie nur diese Einstellungen vornehmen und SuSE-Firewall verwenden, ist Ihr System aber noch keineswegs per se sicher!

Um die Sicherheit eines Firewall-Servers weiter zu erhöhen, sollten Sie:

- Alle Dienste an unsichere Netze (z. B. das Internet) minimieren, nur als sicher geltende Programme verwenden (z. B. postfix, ssh etc.) und diese sorgfältig konfigurieren. Zudem müssen Sie darauf hoffen, dass diese Programme wirklich keine Sicherheitslöcher aufweisen. Alle Dienste sollten möglichst *NICHT* unter `'root'` aufgeführt werden und außerdem in einem "chroot"-Umfeld laufen.
- Vertrauen Sie keiner Software, die Sie nicht selbst geprüft haben.
- Prüfen Sie regelmäßig die Integrität des Servers.
- Wenn Sie, was nicht empfehlenswert ist, den Firewall/Bastion-Server als Masquerading- oder als Routing-Server verwenden wollen, sollten Sie prüfen, ob nicht Proxy-Dienste genutzt werden können, z. B. Squid für das WWW, smtpd für Mail etc. Denken Sie auch hier bitte an "chroot" und lassen Sie die Prozesse nicht unter `'root'` laufen. Stellen Sie das Routing auf dieser Maschine ab.

Im Folgenden finden Sie Erläuterungen zur Konfigurationsdatei des SuSE-Firewall-Skriptes: `/etc/rc.config.d/firewall.rc.config`.

Wie bereits beschrieben, müssen Sie diese Datei nicht von Hand erstellen. Benutzen Sie das Firewall Administrations-System auf dem SuSE Firewall Adminhost. Falls Sie jedoch diese Datei für Ihre Zwecke editieren, lesen Sie unbedingt die Dokumentation des Firewall-Skripts und überprüfen Sie Ihr Skript genauestens, bevor Sie es einsetzen. Für eine selbst erstellte Konfiguration können keine Gewährleistung und kein Support in Anspruch genommen werden.

Hinweis

Die Konfiguration dieser Einstellungen und die Benutzung des SuSE-Firewall-Skripts alleine macht Ihr System nicht von Haus aus sicher. Es gibt *NICHTS*, was sich einfach installieren lässt und Sie vor allen Sicherheitslücken schützt.

Für ein „sicheres“ System sollten Sie außerdem folgendes beachten:

Sichern Sie alle an nicht vertrauenswürdigen Netzen (z. B. Internet) angebotenen Dienste durch die Verwendung von Software, die in Hinblick auf Sicherheit entwickelt worden sind (z. B. postfix und ssh). Setzen Sie keine Software ein, die aus nicht-vertrauenswürdigen Quellen stammt. Darüber hinaus sollten Sie regelmäßig die Sicherheit Ihres Servers überprüfen.

Konfiguration des SuSE-Firewall-Skripts

Um das Firewall-Skript starten zu können, muss auf jeden Fall die Variable `START_FW` in der Datei `/etc/rc.config` auf "yes" gesetzt sein. Bei der Verwendung des SuSE Firewall Adminhosts geschieht dies automatisch.

Wenn es sich bei diesem Rechner um eine Firewall handelt, die wie ein Proxy funktioniert (also kein Routing zwischen den Netzwerken), oder wenn Sie Enduser sind, der gleichzeitig mit dem Internet und dem Intranet verbunden ist, müssen Sie die Punkte 2), 3), 9) und evtl. 7), 10), 11), 12), 14) und 18) konfigurieren.

Wenn der Rechner als Firewall dient und die Funktionalität von Routing bzw. Masquerading zur Verfügung stellen soll, dann müssen Sie die Punkte 2), 3), 5), 6), 9), und evtl. 7), 10), 11), 12), 15), 18) bearbeiten.

Wenn Sie genau wissen, was Sie tun, können Sie die Punkte 8), 16), 17), 18) und die Experten-Optionen 20) 21) und 22) am äußersten Ende der Datei umkonfigurieren. SuSE empfiehlt jedoch, davon Abstand zu nehmen.

Wenn Sie „diald“ oder „ISDN dial-on-demand“ benutzen möchten, sollten Sie den Punkt 18) setzen.

Um Programme wie **`traceroute`** mit Ihrer Firewall zusammen zu verwenden, müssen Sie die folgenden Optionen auf „yes“ setzen: 11 (nur UDP), 19 und 20.

Wenn Sie alle Paketfilter-Regeln selbst dann laden wollen, wenn sie noch nicht verfügbar sind, dann konfigurieren Sie eine statische IP und Netzmaske dafür. Beachten Sie die Beispiele unter 2), 3) und 4).

Bitte beachten Sie, wenn Sie Service-Namen verwenden, dass diese in `/etc/services` stehen. Es gibt z. B. keinen Service „DNS“, die richtige Bezeichnung ist „domain“; E-Mail heißt „smtp“ usw.

Jedes Routing zwischen Interfaces mit Ausnahme von Masquerading verlangt, dass **`FW_ROUTE`** auf `yes` gesetzt ist. Außerdem verwenden Sie die Variablen **`FW_FORWARD_TCP`** und/oder **`FW_FORWARD_UDP`**.

1. Soll das Firewall-Skript beim Systemboot gestartet werden?

   Hierfür muss die Variable **`START_FW`** in `/etc/rc.config` auf "yes" gesetzt werden.

2. Welche Netzwerkinterfaces sind mit dem Internet oder nicht vertrauenswürdigen Netzwerken verbunden?

   Geben Sie hier alle Netzwerke an die nicht vertrauenswürdig sind. Sie können beliebig viele Interfaces durch Leerzeichen getrennt angeben, z. B. "eth0" oder "ippp0 ippp1".

FW_DEV_WORLD=""

Sie können eine statische IP-Adresse und eine Netzwerkmaske angeben, um damit das Laden einer Paketfilter-Regel für ein Interface zu erzwingen, das noch nicht zur Verfügung steht.

FW_DEV_WORLD_[device]="IP_ADDRESS NETMASK"

Sie müssen trotzdem zuerst **FW_DEV_WORLD** definieren! Der Eintrag sieht dann z. B. so aus:

FW_DEV_WORLD_ippp0="10.0.0.1 255.255.255.0"

3. Welche Netzwerkinterfaces sind mit dem internen Netzwerk verbunden?

   Geben Sie alle Netzwerk-Devices an, die vertrauenswürdig sind. Wenn Sie nicht mit einem vertrauenswürdigen Netzwerk verbunden sind, (z. B. wenn Sie nur eine Dialup-Verbindung haben) dann lassen Sie die Liste leer. Sie können wieder beliebig viele Netzwerk-Devices durch Leerzeichen getrennt angeben, also z. B. "eth0" oder "eth0 eth1 ippp0".

   FW_DEV_INT=""

   Sie können eine statische IP-Adresse und eine Netzwerkmaske angeben, um damit das Laden einer Paketfilter-Regel für ein Interface zu erzwingen, das noch nicht zur Verfügung steht:

   FW_DEV_INT_[device]="IP_ADDRESS NETMASK"

   Sie müssen aber trotzdem zuerst **FW_DEV_INT** definieren! Siehe dazu das folgende Beispiel für das interne Interface "eth0":

   FW_DEV_INT_eth0="192.168.1.1 255.255.255.0"

4. Welches Interface zeigt auf die DMZ?

   Geben Sie alle Netzwerkdevices an, die auf die DMZ zeigen. Achtung: Konfigurieren Sie die Variablen **FW_FORWARD_TCP** und **FW_FORWARD_UDP**, um die Dienste anzugeben, die dem Internet zur Verfügung stehen sollen, und setzen Sie die Variable **FW_ROUTE** auf "yes". Sie können z. B. wählen zwischen: "tr0", "eth0 eth1" oder "".

   FW_DEV_DMZ=""

   Sie können eine statische IP-Adresse und eine Netzwerkmaske angeben, um damit das Laden einer Paketfilterregel für ein Interface erzwingen, das noch nicht zur Verfügung steht.

   FW_DEV_DMZ_[device]="IP_ADDRESS NETMASK"

   Sie müssen trotzdem zuerst **FW_DEV_DMZ** definieren! Siehe dazu das folgende Beispiel für das DMZ-Interface "eth1"

   FW_DEV_DMZ_eth1="192.168.1.1 255.255.255.0"

5. Soll „Routing“ zwischen dem Internet, der DMZ und dem internen Netzwerk aktiviert werden? Dazu brauchen Sie **FW_DEV_INT** oder **FW_DEV_DMZ**.

   Sie müssen nur die Variable auf "yes" setzen, wenn Sie entweder interne Maschinen maskieren wollen oder Zugriff auf die DMZ erlauben wollen. Diese Option überschreibt die Variable **IP_FORWARD** in `/etc/rc.config`.

Wenn Sie diese Option setzen, passiert noch gar nichts. Entweder aktivieren Sie Masquerading mit der Variable **FW_MASQUERADE** weiter unten, oder Sie konfigurieren **FW_FORWARD_TCP** und/oder **FW_FORWARD_UDP**, um zu definieren, was geroutet wird. Sie können hier nur "yes" oder "no" angeben, Standard ist "no".

FW_ROUTE="no"

6. Wollen Sie interne Netzwerke nach außen maskieren? Benutzen Sie dazu **FW_DEV_INT** und **FW_ROUTE**.

   „Masquerading“ bedeutet, dass alle Ihre internen Rechner, die Dienste des Internets benutzen, scheinbar von der Firewall aus kommen. Beachten Sie, dass es sicherer ist, über Proxies mit dem Internet zu kommunizieren als Masquerading einzusetzen.

   Wahlmöglichkeit: "yes" oder "no", Standard: "no"

   FW_MASQUERADE="no"

   Welche internen Rechner/Netzwerke sollen Zugriff auf das Internet haben? Nur diese Netzwerke dürfen ins Internet und werden maskiert. Lassen Sie die Liste leer oder geben Sie beliebig viele Netzwerke/Rechner durch Leerzeichen getrennt an, jedem Netzwerk/Host können Sie zusätzlich durch ein Komma getrennt Protokolltyp und Dienst anfügen.

   FW_MASQ_NETS=""

   Geben Sie zusätzlich das Interface an, auf dem das Maskieren stattfinden soll, z. B. "ippp0" oder "$FW_DEV_WORLD"
   FW_MASQ_DEV="$FW_DEV_WORLD"

7. Wollen Sie die Firewall vor den internen Netzwerken schützen? Das erreichen Sie mit **FW_DEV_INT**. Ist diese Variable auf "yes" gesetzt, können interne Computer nur die von Ihnen freigegebenen Dienste nutzen.

   Auswahlmöglichkeit: "yes" oder "no", Grundeinstellung: "yes"

   FW_PROTECT_FROM_INTERNAL="yes"

8. Wollen Sie alle global laufenden Dienste schützen?

   Wenn Sie hier "yes" angeben, werden alle Netzwerk-Zugriffe auf TCP und UDP auf diesem Rechner verhindert, die nicht an eine bestimmte IP-Adresse gebunden oder explizit zugelassen sind. Siehe **FW_*SERVICES_***. "0.0.0.0:23" wird z. B. geschützt, "10.0.0.1:53" nicht. Auswahl: "yes" oder "no", default ist "yes".

   FW_AUTOPROTECT_GLOBAL_SERVICES="yes"

9. Welche Dienste auf dem **Firewall-Rechner** sollen vom Internet oder anderen nicht vertrauenswürdigen Netzwerken, der DMZ oder dem Internen Netz aus zugänglich sein? (Siehe Nr.13 & 14, wenn Sie Netzwerkverkehr durch die Firewall routen wollen.) Geben Sie alle Port-Nummern oder -Namen getrennt durch Leerzeichen an. TCP basierte Dienste (z. B. SMTP, WWW) müssen in **FW_SERVICES_*_TCP** – und in **FW_SERVICES_*_UDP** müssen UDP-Dienste (syslog) gesetzt werden. Für IP-Protokolle (wie GRE für PPTP oder OSPF für Routing) müssen Sie **FW_SERVICES_*_IP** mit dem

Protokoll-Namen oder der Protokoll-Nummer (vgl. `/etc/protocols`) angeben.

Auswahlmöglichkeiten: Leere Liste oder jede Portnummer, Portnamen (vgl. `/etc/services`) oder Port-Bereiche (z. B. 1024:2000) durch Leerzeichen getrennt oder Dienste (TCP), die von extern aus sichtbar sein sollen, normalerweise „smtp domain“.

`FW_SERVICES_EXTERNAL_TCP=""`

Dienste (UDP), die von Extern aus sichtbar sein sollen, üblicherweise „domain“:

`FW_SERVICES_EXTERNAL_UDP=""`

Dienste (andere) die für die DMZ sichtbar sein sollen, z. B. VPN/Routing das an der Firewall endet:

`FW_SERVICES_EXTERNAL_IP=""`

Dienste (TCP), die für die DMZ sichtbar sein sollen, normalerweise „smtp domain“:

`FW_SERVICES_DMZ_TCP=""`

Dienste (UDP), die für die DMZ sichtbar sein sollen, normalerweise „domain syslog“:

`FW_SERVICES_DMZ_UDP=""`

Dienste (andere), die für die DMZ sichtbar sein sollen, z. B. VPN/Routing das an der Firewall endet:

`FW_SERVICES_DMZ_IP=""`

Dienste (TCP), die für das interne Netz sichtbar sein sollen, normalerweise „ssh smtp domain“:

`FW_SERVICES_INTERNAL_TCP=""`

Dienste (UDP), die für das interne Netz sichtbar sein sollen, normalerweise „domain syslog“:

`FW_SERVICES_INTERNAL_UDP=""`

Dienste (andere), die für die DMZ sichtbar sein sollen, z. B. VPN/Routing das an der Firewall endet:

`FW_SERVICES_INTERNAL_IP=""`

10. Welche Dienste sollen von vertrauenswürdigen Netzen aus dem Internet erreichbar sein?

    Geben Sie die vertrauenswürdigen Netze innerhalb des Internets an und die TCP/UDP-Dienste, die sie verwenden dürfen.

    Auswahlmöglichkeiten: leere Liste oder jede beliebige IP-Adresse und/oder Netzwerke durch Leerzeichen getrennt.

    `FW_TRUSTED_NETS=""`

    Geben Sie bei **`FW_SERVICES_TRUSTED_*`** eine leere Liste an, oder die Port-Nummern bzw. die bekannten Portnamen (vgl. `/etc/services`), oder die Portbereiche durch ein Leerzeichen getrennt, z. B. "25", "ssh", "1:65535", "1 3:5"

Dienste (TCP), die vertrauenswürdigen Netzen/Rechnern zur Verfügung gestellt werden sollen, normalerweise „ssh“:

FW_SERVICES_TRUSTED_TCP=""

Dienste (UDP), die vertrauenswürdigen Netzen/Rechnern zur Verfügung gestellt werden sollen, normalerweise „syslog time ntp“:

FW_SERVICES_TRUSTED_UDP=""

Dienste (andere), die für vertrauenswürdige Hosts sichtbar sein sollen, z. B. VPN/Routing, das an der Firewall endet:

FW_SERVICES_TRUSTED_IP=""

Manchmal sollen bestimmte vertrauenswürdige Rechner Zugriff auf bestimmte Dienste haben und andere vertrauenswürdige Rechner auf andere Dienste. Hier haben Sie die Möglichkeit dieses einzurichten, nach dem Muster: "trusted_net,protocol,port", also z. B. "10.0.1.0/24,tcp,80 10.0.1.6,tcp,21":

FW_SERVICES_TRUSTED_ACL=""

11. Ist der Zugriff auf die hohen, unprivilegierten (>1023) Ports erlaubt?

    Sie können jedem den Zugriff auf die hohen Ports erlauben ("yes"), oder allen verbieten ("no"); oder Sie geben jedem, der von einem bestimmten Port kommt (Angabe von Port-Nummer oder Service-Name, was allerdings leicht zu umgehen ist) oder nur den von Ihnen zugelassenen Nameservern (DNS) Zugriff.

    Wenn Sie aktives FTP zulassen wollen, müssen Sie die TCP-Variable auf "ftp-data" setzen. Bei passivem FTP ist das nicht notwendig. Beachten Sie weiterhin, dass Sie keine rpc-Requests benutzen können. Wenn Sie dieses erlauben wollen, müssen Sie in **FW_SERVICES_EXTERNAL_UDP** den Port-Bereich "600:1023" setzen.

    Auswahlmöglichkeiten: "yes", "no", "DNS", Port-Nummer oder Portname, Standard ist "no".

    Eingehende Verbindungen auf port-Nummern >= 1024, TCP, üblicherweise: "ftp-data" (leider!):

    FW_ALLOW_INCOMING_HIGHPORTS_TCP="yes"

    Eingehende Verbindungen auf port-Nummern >= 1024, UDP, üblicherweise: "DNS" oder "domain ntp":

    FW_ALLOW_INCOMING_HIGHPORTS_UDP="yes"

12. Haben Sie einen oder mehrere der folgenden Dienste laufen? Diese benötigen besondere Sorgfalt, oder sie funktionieren nicht. Für Dienste, die Sie anbieten wollen, setzen Sie die Variablen auf "yes" alle anderen auf "no". Default-Werte sind "no".

    FW_SERVICE_DNS="no"
    Im Falle von "yes", **FW_SERVICES_*_TCP** muss port 53 (oder domain) haben. Die Variable **FW_ALLOW_INCOMING_HIGHPORTS_UDP** muss auch auf "yes" gesetzt sein.

    FW_SERVICE_DHCLIENT="no"
    Wenn Sie dhclient benutzen, um eine IP-Adresse zu erhalten, muss **FW_SERVICE_DHCPD** auf "yes" gesetzt werden.

FW_SERVICE_DHCPD="no"
Ist dieser Rechner ein DHCP-Server, dann setzen Sie **FW_SERVICE_DHCPD** auf "yes".

FW_SERVICE_SAMBA="no"
Wenn Sie Samba als Client oder Server auf diesem Rechner verwenden wollen, dann setzen Sie **FW_SERVICE_SAMBA** auf "yes".

Für einen Samba-Server muss zusätzlich noch **FW_SERVICES_{WORLD,DMZ,INT}_TCP="139"** gesetzt sein. Es ist grundsätzlich keine gute Idee, Samba auf einem Firewall-Rechner einzusetzen.

13. Welche Dienste, die vom Internet erreichbar sein sollen, dürfen Zugriff auf die DMZ oder das interne Netzwerk haben?

    Mit dieser Option können Sie den z. B. den Zugriff für Ihren Mailserver erlauben. Diese Rechner müssen eine gültige IP-Adresse haben. Es wird eine offene Verbindung zu Ihrem Netzwerk aufgebaut, benutzen Sie diese Option daher nur für Zugriffe auf Ihre DMZ. Folgende Werte sind möglich: Lassen Sie die Variable leer (die beste Wahl) oder verwenden Sie die folgende Syntax für die Forwarding-Regeln. Die Regeln trennen Sie durch Leerzeichen.

    Eine Forwarding-Regel besteht aus:

    a) Quell-IP/Netz,
    b) Ziel-IP (dmz/intern),
    c) Ziel-Port (oder IP protocol), getrennt durch Komma

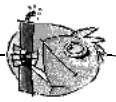
```
# Forward TCP connections
# Beware to use this!
FW_FORWARD_TCP=""
# Forward UDP connections
# Beware to use this!
FW_FORWARD_UDP=""
# Forward other IP protocol connections (for VPN setups)
# Beware to use this!
FW_FORWARD_IP=""
```

14. Welche Dienste dürfen auf maskierten Rechner (in Ihrer DMZ oder dem internen Netz) verwendet werden?

    REQUIRES: FW_ROUTE, FW_MASQUERADE

    Mit diesen Variablen können Sie den Zugang z. B. auf Ihren Mailserver gestatten. Die Rechner müssen in einem maskierten Netzsegment stehen und dürfen keine offiziellen IP-Adressen haben.

    Wenn **FW_DEV_MASQ** auf Ihr externes Interface gesetzt ist, müssen Sie auch die Variablen **FW_FORWARD_*** von Ihrem internen Netzwerk in die DMZ für diese Dienste auch setzen.



Achtung

Aus Sicherheitsgründen sollten Sie diese Funktionalität nicht verwenden. Sie öffnen damit ein Sicherheitsloch in Ihrem internen Netzwerk. Wenn z. B. Ihr Webserver kompromittiert wird, ist Ihr gesamtes Netzwerk ebenfalls unsicher.

Wahlmöglichkeiten: Lassen Sie den Eintrag leer (beste Wahl) oder verwenden Sie folgende Syntax für die Forwarding-Masquerade-Regeln. Die Regeln werden durch Leerzeichen getrennt.

a) Quell-IP/Netz,

b) Ziel-IP (dmz/intern)

c) Ziel-Port, getrennt durch Kommata,
z. B.: "4.4.4.4/12,20.20.20.20,22 12.12.12.12/12,20.20.20.20,22"

```
# Forward TCP connections to masqueraded host
# Beware to use this!
FW_FORWARD_MASQ_TCP=""
# Forward UDP connections to masqueraded host
# Beware to use this!
FW_FORWARD_MASQ_UDP=""
# it is not possible to masquerade other IP protocols,
# hence no _IP variable
```

15. Welche Dienste sollen auf einen lokalen Port auf dem Firewall-Rechner umgelenkt werden?

    Dies kann dazu verwendet werden, alle Ihre internen Benutzer über Ihren HTTP-Proxy zu leiten oder transparent alle eingehenden Anfragen auf Port 80 an einen sicheren Webserver weiterzuleiten.

    Auswahl: Lassen Sie die Liste leer oder verwenden Sie die folgende Syntax für die redirecting rules:

    a) Quell-IP/Netz,

    b) Ziel-IP/Netz,

    c) ursprünglicher Bestimmungsport,

    d) lokaler Port auf den der Netzwerkverkehr umgebogen werden soll,
    z. B.: "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"

```
 Redirect TCP connections
FW_REDIRECT_TCP=""
 Redirect UDP connections
FW_REDIRECT_UDP=""
```

16. Welcher Log-Level soll erzwungen werden?

    Sie können angeben, ob Pakete, die angenommen oder abgelehnt werden, geloggt werden. Sie können außerdem den Log-Level angeben, "critical" oder alles. Beachten Sie, dass ***_ALL** nur für Debugging-Zwecke aktiviert werden sollte.

    Möglichkeiten für die Variable: "yes" oder "no", **FW_LOG_*_CRIT** Standard ist "yes".

```
# Log critical denied network packets
FW_LOG_DENY_CRIT="yes"
# Log all denied packets
FW_LOG_DENY_ALL="no"
# Log critical accepted packets
FW_LOG_ACCEPT_CRIT="yes"
# Log all accepted packets
FW_LOG_ACCEPT_ALL="no"
```

17. Wollen Sie zusätzliche Kernel TCP/IP Sicherheits-Features? Wenn Sie diese Variable auf "yes" setzen, werden die folgenden Kerneloptionen gesetzt:

    ```
    icmp_ignore_bogus_error_responses,
    icmp_echoreply_rate,
    icmp_destunreach_rate,
    icmp_paramprob_rate,
    icmp_timeexeed_rate,
    ip_local_port_range,
    log_martians,
    mc_forwarding,
    rp_filter,
    routing flush
    ```

    Auswahlmöglichkeiten: "yes" oder "no", default ist "yes":
    `FW_KERNEL_SECURITY="yes"`

18. Soll das Routing eingeschaltet bleiben, wenn die Paketfilterregeln zurück gesetzt werden? Dazu benötigen Sie **`FW_ROUTE`**.

    Wenn Sie „diald“ oder „dial-on-demand“ via ISDN verwenden und IP-Pakete in das Internet geschickt werden sollen, müssen Sie diese Funktion einschalten. Masquerading und Routing werden dann vom Skript nicht ausgeschaltet, wenn es beendet wird. Es kann sein, dass Sie diese Funktionalität brauchen, wenn Sie eine DMZ haben. Bedenken Sie allerdings, dass das **unsicher** ist! Wenn Sie die IP-Filterregeln entladen und immer noch eine Verbindung haben, kann Ihr Netzwerk für Attacken offen liegen.

    Auswahl: "yes" oder "no", Default-Einstellung: "no"

    `FW_STOP_KEEP_ROUTING_STATE="no"`

19. Sollen ICMP echo pings auf den Firewall-Rechner oder die DMZ erlaubt sein? Benötigt wird **`FW_ROUTE`** für **`FW_ALLOW_PING_DMZ`**

    Auswahl: "yes" oder "no", Voreinstellung ist "no"

```
# Erlaube ping auf Firewall
FW_ALLOW_PING_FW="yes"
# Erlaube ping auf DMZ Rechner.
FW_ALLOW_PING_DMZ="yes"
```

Erstellung eines eigenen Paketfilters mit ipchains

Wenn Sie nicht das SuSE Firewall-Skript verwenden wollen, haben Sie auch die Möglichkeit, einen eigenen Paketfilter mit ipchains zu konfigurieren. Sie

erstellen die Filterregeln nach Ihren Bedürfnissen auf einem Linux-Rechner, z. B. dem SuSE-Firewall-Adminhost, und speichern dieses Paket-Filter-Setup mit ipchains-save in eine Datei.

```
root@adminhost # ipchains-save > myfiltersetup 2>/dev/null
```

Mit FAS laden Sie dann diese Datei mit Ihrer Paketfilter-Konfiguration in die Konfiguration der „SuSE Linux Live-CD for Firewall“. Diese Filterregeln werden in der Datei `/etc/ipchainsrc` auf der Konfigurationsdiskette gespeichert und vom Skript `/sbin/init.d/ipchains` beim Boot-Vorgang des Firewall-Rechners geladen.

5.3.2 DNS

Um die Namensauflösung durch die Firewall zu ermöglichen, wird der Nameserver BIND Version 8 eingesetzt. Wenn Sie mehr über DNS erfahren möchten, lesen Sie bitte das Kapitel im Anhang dieses Handbuchs. BIND wird als forwarding/caching-only Server konfiguriert. Das heißt, es werden alle Anfragen an die Forwarders weitergeleitet.

5.3.3 MAIL

postfix

Sicherer, schneller und flexibler modular aufgebauter Mail-Transport-Agent, der auf der Live-CD als Mail-Relay zum Einsatz kommt. Zu beachten ist, dass für die Verwendung der Mailrelay-Funktion eine eingebaute Festplatte unbedingt erforderlich ist, weil postfix die eingehenden E-Mails zunächst zwischenspeichern muss.

5.3.4 HTTP-Proxy

Um eine möglichst feingranulierte Steuerung des Zugriffs auf HTTP/HTTPS-Dienste zu ermöglichen, verwendet die „SuSE Linux Live-CD for Firewall“ eine Kaskade von verschiedenen Proxies. Für Zugriffe von intern nach extern und von extern nach intern werden zwei getrennte Proxy-Instanzen verwendet.

squid

Squid ist der „http-proxy“ schlechthin und bietet umfangreiche Konfigurationsmöglichkeiten sowie die Steuerung des Zugriffs von Clients auf das WWW mittels ACLs (engl. *access control lists*).

Der interne HTTP-Proxy Squid kann transparent oder nicht transparent konfiguriert werden. Im *nicht-transparenten* Modus werden folgende Protokolle unterstützt:

- http
- https

- FTP

Voraussetzung ist dabei, dass die Clients (Webbrowser) diesen Proxy auch in den Einstellungen als Proxy eingetragen haben.

Hinweis

Squid kann aber nur HTTP transparent verarbeiten! Transparentes HTTPS oder FTP funktioniert nicht mit Squid.
Für Transparentes HTTPS gibt es zur Zeit keine Lösung, außer es wird direkt durch die Firewall durchgeschleust.
Für transparentes FTP kann die Proxy-Suite (interns FTP im FAS) benutzt werden.

Genauere Informationen zu Squid finden Sie im Anhang.

httpf, tinyproxy

Das Programm httpf ist für das "content filtering" zuständig. Es ist kein Proxy im eigentlichen Sinne, denn die Proxy-Funktionalität wird über das Programm tinyproxy erbracht.

Es handelt sich vielmehr um einen filternden Proxy, der das Herunterladen und die Ausführung von Programmcode verhindern kann. Dies geschieht, indem nur bekannte, ungefährliche Sprachelemente an den Webbrowser weitergeleitet werden. Auch die Einträge in den HTTP-Köpfen können gefiltert werden, so dass z. B. keine Informationen über das Betriebssystem des Client-Rechners an den Server übergeben werden.

Die Konfiguration erzeugen Sie mit FAS auf dem Adminhost.

transproxy

transproxy regelt den Zugriff von extern auf einen internen Webserver.

Diese Programme insgesamt bieten die Möglichkeit, vielfältig zu filtern: ACLs für Clients, Server, Banlists, Contentfiltering, Webcaching.

5.3.5 FTP-Proxy

Der FTP-Dienst wird in zwei Richtungen aufgeteilt. Erstens: Verbindungsaufbau von intern nach extern und zweitens: Verbindungsaufbau von extern nach intern/DMZ.

Von intern nach extern:

magic-user

Ermöglicht die Angabe des Usernamens, des Hosts und des Ports des Ziel-FTP-Servers (z. B. `user@ftp.firma.com:2345`). Also automatisches Ausführen des USER-Kommandos.

Von extern nach intern:

Falls Sie einen FTP-Server betreiben möchten, definieren Sie in diesem Teil des Moduls die Einstellungen, um auf den FTP-Server einen Zugriff aus dem Internet zu ermöglichen.

Proxy Konfiguration für einen eigenen FTP-Server

IP-Adresse des FTP-Servers: IP-Adresse Ihres FTP-Servers in Ihrer DMZ (oder Intranet), der vom Internet aus zugänglich sein soll.

FTP-Proxy-Port: Normalerweise 21 (voreingestellt).

Maximale Anzahl von Clients: Die maximale Anzahl an offenen Verbindungen ist auf 512 begrenzt (standardmäßig 64).

Höre auf ausgewählte IP-Adresse: IP-Adresse des Interfaces, auf dem der FTP-Server die Anfragen für Verbindungen vom Internet entgegennehmen soll. '`0.0.0.0`' steht für alle Interfaces, die die Firewall hat.

Hinweis

Der FTP-Proxy öffnet seine Datenkanäle für externe Clients in dem Bereich der Portnummern 41000 bis 41999. Beachten Sie dies bei der Konfiguration ihres Paketfilters.

Port reset PASV: Es gibt zwei Möglichkeiten, um zu einem FTP-Server eine Verbindung herzustellen:

- aktiver FTP-Modus: bei einer Anfrage öffnet der Server einen Port für den Datentransfer.
- passiver FTP-Modus (PASV): dem Server wird die Port-Nr. mitgeschickt, auf dem die Daten empfangen werden sollen.

Identische Adresse: Ist die Option aktiviert ('`yes`', Standardeinstellung), wird erzwungen, dass der Server, an den die Anfrage gestellt wurde (und kein anderer), diese auch beantwortet.

5.3.6 ssh

openssh ermöglicht die Verwendung einer Shell auf einem entfernten Rechner, wobei die Verbindung verschlüsselt wird.

5.3.7 chroot, secumod, compartment, Kernel-capabilities

Um die Sicherheit auf der Firewall zu erhöhen, laufen auf der SuSE Live-CD for Firewall die Dienste in einer `chroot`-Umgebung. Außerdem werden das „secumod“-Kernelmodul und „compartment“ verwendet. Durch das Setzen von Capability-Bits im Kernel wird die Sicherheit von Programmen im System erhöht.

chroot Mit chroot kann ein Programm seine Sicht auf das Dateisystem unwiderruflich ändern, indem es sich eine neue "root" für das Dateisystem festlegt. Sobald sich das Programm auf den Ausschnitt des Dateisystems festgelegt hat, übernimmt dieser Ausschnitt die Rolle des gesamten Dateisystems für dieses Programm. Das übrige Dateisystem existiert aus der Sicht des Programms nicht mehr. Selbst wenn das Programm irgendwie crashed, bleibt der Angreifer in dieser chroot-Umgebung und kann das eigentliche System nicht beschädigen.

secumod Spezielles Kernelmodul, mit dem die Sicherheit des Systems erhöht wird. Dazu gehört z. B.: das Festlegen von

- Trusted Path,
- Verbot von Hardlinks auf Dateien anzulegen, die einem nicht gehören,
- Schutz des proc-Filesystems,
- Symlinks werden nicht verfolgt, wenn sie nicht dem gerade laufenden Prozess (Ausnahme: der Prozess läuft unter `'root'`-Rechten) gehören.
- Schutz von fifos,
- syscall table checking,
- logging,
- Setzen von Capabilities.

compartment Ermöglicht das Laufen von Programmen/Diensten in chroot-jails mit unprivilegierten Benutzern/Gruppen. Es unterstützt Skripte, die vor dem eigentlichen Programmstart aufgerufen werden (z. B. zum Aufbau einer chroot-Umgebung). Unterstützt die Verwendung von Kernelcapabilities.

Kernelcaps Capability-Bits des Kernels

Erhöhung der Sicherheit durch Begrenzung der Fähigkeiten des ausführbaren Programms.

Die Capabilities sind unter

`/usr/include/linux/capability.h`

dokumentiert.

Eine relativ einfache Möglichkeit die Capabilities für ein Programm anzugeben, ist die Verwendung des Programms compartment.

5.4 Die Konfigurationsdiskette

Auf der Konfigurationsdiskette ist die komplette Systemkonfiguration und die Konfiguration der Applications-Level-Gateways enthalten.

Die Konfigurationsdiskette muss mit einem ext2-Dateisystem versehen werden und mit folgendem Befehl das Label "SuSE-FWFloppy" erhalten:

Legen Sie eine mit ext2-Dateisystem formatierte Diskette ein.

`/sbin/e2label/dev/fd0SuSE-FWFloppy`

Ohne dieses Label wird die Konfigurationsdiskette nicht erkannt. Das FAS (Firewall Administration System) auf dem SuSE Linux Firewall Adminhost erzeugt das Dateisystem und das Label automatisch.

Die Konfigurationsdiskette wird während des Bootens der Live-CD eingelesen.

5.4.1 Erstellen der Konfigurationsdiskette

Die Konfigurationsdiskette lässt sich auf dem SuSE Linux Firewall Adminhost mit der Adminstrations-Oberfläche FAS erzeugen. Das FAS auf dem SuSE Linux Firewall Adminhost erzeugt ein tar-Archiv, das dann auf Diskette entpackt wird. Das ist die empfohlene Methode. Die Konfigurationsdateien mit einem Editor zu bearbeiten ist nur für Experten ratsam, die wirklich wissen was sie tun Es gibt hierfür auch keinen Support.

5.4.2 Die Konfigurationsdateien

Die folgende Übersicht über die Konfigurationsdateien, die sich auf der Diskette befinden, dient nur Ihrer Information; die Dateien werden mit der Admin-Oberfläche erstellt:

/etc/hosts (vgl. man hosts)
/etc/hosts.allow (vgl. man 5 hosts_access)
/etc/hosts.deny (vgl. man 5 hosts_access)
/etc/inittab (man inittab)
/etc/isdn/
/etc/cipe/
/etc/live-setup.conf
/etc/passwd
/etc/ppp/
/etc/localtime
/etc/modules.boot

In der Datei `/etc/modules.boot` können Sie ladbare Kernelmodule angeben, die beim Systemstart geladen werden sollen. Sie werden mit dem relativen Pfadnamen zum Verzeichnis `/lib/modules/<Kernelversion>/` angegeben. Falls nötig, können auch noch Optionen an das Modul übergeben werden, wie z. B. IRQ oder IO-Adresse der verwendeten Hardware. Zeilen die mit "#" beginnen, werden ignoriert. Stellt man dem Modulnamen ein "-" voran, so wird

versucht, das Modul zu entladen (dies kann notwendig werden, falls die automatische Hardwareerkennung z. B. ein falsches Netzwerkmodul zu laden versucht).

Beispiel:

```
# In this file you can provide a list of modules
# and options, that have to be loaded on system boot.
# Module-Name can be used relative, i.e. net/ppp.o.
#
# Module-Name [Options]
#
#  z. B.:
#misc/cipcb.o
#net/slhc.o
#net/ppp.o
#net/ppp_deflate.o
#net/ppp_mppe.o
-net/de4x5.o   # Dieses Modul wird entfernt
 net/tulip.o    # Dieses Modul wird geladen
```

/etc/ipsec.d/ enthält Zertificate und Konfigurationsdateien.

/etc/named/ enthält die Zone-Files des Nameservers.

/etc/named/master/ enthält die Master-Zone-Files.

/etc/named/slave/ enthält die Slave-Zone-Files.

/etc/named/root.hint enthält die Adressen der root-Nameserver.

/etc/named.conf hier erfolgt die Konfiguration von named.

/etc/ntp.conf Konfiguration des Timeserver Daemons xntpd

/etc/pam.d/ dieses Verzeichnis enthält die Konfigurationsdateien von PAM (engl. *Pluggable Authentication Module*).

/etc/permissions.local setzt die Zugriffsrechte von bzw. auf Programme, Dateien usw.

/etc/postfix Konfigurationsverzeichnis für postfix; die Hauptkonfigurationsdateien sind:

- `/etc/postfix/master.cf`,
- `/etc/postfix/main.cf`,
- `/etc/postfix/virtual`,
- `/etc/postfix/transport`,
- `/etc/postfix/access`.

/etc/proxy-suite/ Konfigurationsverzeichnis der FTP-Proxies,

/etc/rc.config SuSE Linux Hauptkonfigurationsdatei;

/etc/rc.config.d/ dieses Verzeichnis enthält weitere Konfigurationsdateien, die von SuSEconfig gelesen werden;

/etc/rc.config.d/firewall.rc.config Konfigurationsdatei für das SuSE Firewall Skript. Diese Datei wird vom FAS auf dem SuSE Linux Adminhost for Firewall erzeugt.

/etc/rinetd.conf Konfigurations Datei für den generischen Proxy rinetd.

/etc/resolv.conf Konfiguration für die Resolver-Bibliothek, Angabe der Nameservers und der Searchlist.

/etc/route.conf Datei, welche die Informationen für die Erstellung der statischen Kernelroutingtabelle enthält.

/etc/runlevel.firewall Hier findet eine Zuordnung von Skripten/Programmen zu den Runlevels der Firewall statt. Wenn ein Skript in einem bestimmten Runlevel aufgerufen werden soll, dann trägt man es in die entsprechende Spalte der Datei ein.

/etc/securetty Die Liste der tty, auf denen sich der Benutzer `'root'` anmelden kann.

/etc/shadow Enthält die verschlüsselten Passwörter. Normalerweise ist dies für alle Benutzer ein „*“, das heißt, es ist kein Login möglich. Nur für den Benutzer `'root'` ist hier ein verschlüsseltes Passwort hinterlegt. Es besteht auch die Möglichkeit, in FAS kein `'root'`-Passwort anzugeben. Dann ist ein Zugang zur Firewall nur über SSH- und RSA-Schlüssel möglich.

/etc/squid.conf Konfigurationsdatei für den HTTP-Proxy Squid.

/etc/ssh/ Enthält die Konfigurationsdateien für openssh: `ssh_config` und `sshd_config`.

/etc/su1.priv Konfigurationsdatei für das Kommando **su1**, das ausgewählten Benutzern das Ausführen von Programmen mit der uid=0 (d. h. als `'root'`) ermöglicht.

/etc/syslog.conf Konfiguration des Syslog-Daemons. Lesen Sie hierzu folgende Man-Pages: **`man 5 syslog.conf`**, **`man 8 syslogd`** und **`man 3 syslog`**.

In dieser Datei wird der Loghost eingetragen und welche Meldungen erfasst werden sollen. Der Eintrag für den Loghost sollte folgendermaßen aussehen:

```
*.*   @hostname.domain.tl  (oder die IP-Adresse)
```

/etc/syslog.socks für alle Dienste, die in der Umgebung `chroot` gestartet werden, muss der Log-Daemon `syslog` einen Socket anlegen, auf den er schreiben kann; dabei handelt es sich um:

```
/var/named/dev/log,
/var/squid/dev/log,
/var/chroot/rinetd/dev/log,
/var/chroot/ftp-intern/dev/log,
/var/chroot/ftp-extern/dev/log
```

/etc/init.d/ Dieses Verzeichnis enthält selbstgeschriebene init-Skripten, z. B. IP-Paketfilter-Skripten.

/root/, /root/.ssh/, /root/.ssh/authorized_keys Enthält den rsa-public key des fwadmin-Benutzer auf dem SuSE Linux Firewall Adminhost.

Damit wird es möglich, dass sich der Benutzer `'fwadmin'` als `'root'` auf der Firewall einloggen kann. Die Authentifizierung findet mittels der RSA-Schlüssel statt, die wiederum mit einer Passphrase geschützt sind. Diese Passphrase wird bei der Installation des Adminhostes mittels des YaST2-Moduls „Firewall Admin Host“ erzeugt.

Sie können die RSA-keys auch auf der Kommandozeile mit dem Befehl **`ssh-keygen(1)`** erzeugen. Lesen Sie dazu auch die Man-Page (**`man ssh-keygen`**).

Es wird nachdrücklich empfohlen, die Konfigurationsdateien mit der Administrationsoberfläche FAS auf dem SuSE Firewall Adminhost zu erstellen.

5.5 Boot-Parameter

Am Boot-Prompt von linuxrc können Sie wie gewohnt Boot-Parameter übergeben (siehe Referenzhandbuch, Kernel-Boot-Parameter).

Es gilt die folgende Einschränkung:

Aus Sicherheitsgründen kann am Boot-Prompt kein `init=/bin/bash` oder Ähnliches angegeben werden, um eine Shell mit privilegierten Rechten zu erhalten.

Boot-Parameter, die mit "init=" beginnen, werden ignoriert.

6 Inbetriebnahme der Firewall

Voraussetzungen für die erfolgreiche Inbetriebnahme:

Sie haben eine Konfiguration für die SuSE Linux Live-CD for Firewall mit dem SuSE Linux Adminhost for Firewall bzw. eine Konfigurations-Diskette von Hand erstellt. Jetzt wird der Firewall-Rechner in mehreren Schritten in Betrieb genommen. Zunächst überprüfen Sie, ob Ihr Rechner mit der bereits erstellten Konfiguration bootet und die ausgewählten Dienste alle starten und verfügbar sind. Anschließend kontrollieren Sie, ob der IP-Filter des Kernels der Konfiguration gemäß arbeitet.

6.1 Booten des Firewall-Rechners

1. Starten Sie den Rechner und öffnen Sie das BIOS-Setup-Programm. Überprüfen Sie Uhrzeit und Datum.
2. Stellen Sie die Bootsequenz so ein, dass der Rechner zuerst von CD bootet – falls möglich nur von CD.
3. Vergeben Sie unbedingt ein BIOS-Passwort. Damit verhindern Sie, dass die Boot-Sequenz geändert und der Firewall-Rechner von Diskette gebootet wird.
4. Speichern Sie die BIOS-Konfiguration ab.
5. Legen Sie die SuSE Linux Live-CD for Firewall ein.
6. Legen Sie die Konfigurations-Diskette ein.
7. Booten Sie den Rechner neu.
8. Achten Sie beim Booten auf Fehlermeldungen und überarbeiten Sie eventuell die entsprechenden Konfigurationsdateien. Wenn Dienste nicht starten (Meldung: "<Dienst xyz> failed/skipped"), liegt ein Fehler in der zugehörigen Konfigurationsdatei für den Dienst <xyz> vor. In diesem Fall erstellen Sie die Konfigurations-Diskette mit dem FAS-Tool auf dem Adminhost neu bzw. überarbeiten die dort abgespeicherte Konfiguration und speichern diese auf der Konfigurationsdiskette erneut ab.

Die Konfiguration der Festplatte haben Sie bereits mit FAS festgelegt. Wenn allerdings die Partitionen 1 (swap) und 2 (var) des Firewall-Rechners nicht mit den Angaben in der Datei `/etc/live-setup.conf` übereinstimmen, erscheint eine Dialog-Maske wie in Abb. 6.1 auf der nächsten Seite. Wenn Sie die Platte neu einrichten möchten, antworten Sie mit ‘`yes`’.

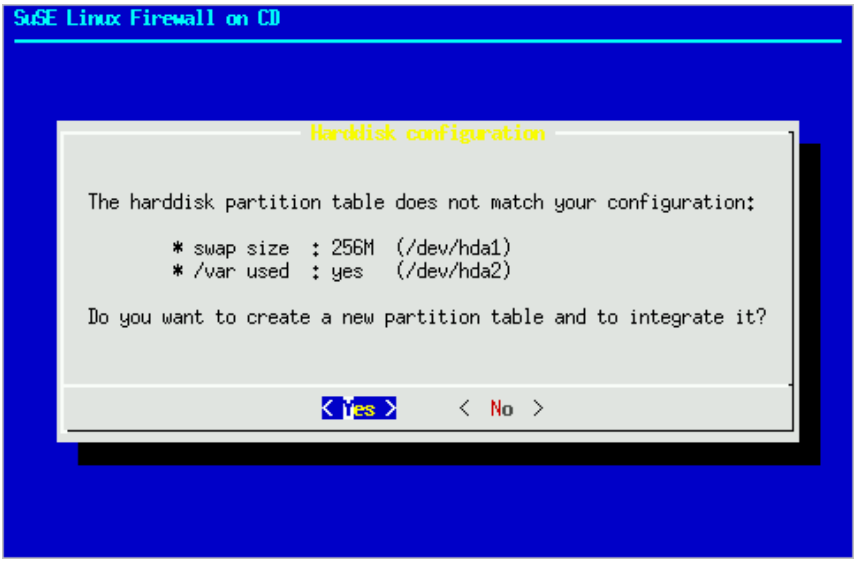


Abbildung 6.1: Dialog zur Konfiguration der Festplatte

6.2 Testen der Firewall

Bevor man die Firewall in Betrieb nimmt, sollte kontrolliert werden, ob erstens der Paketfilter richtig konfiguriert ist und zweitens die konfigurierten Proxies alle starten und die Anfragen richtig bearbeiten. Für diese Zwecke stehen auf dem SuSE Firewall Adminhost Werkzeuge bereit (siehe 3 auf Seite 17) wie nmap, nessus, xlogmaster, logsurfer, http-Clients usw. Für diese Programme gibt es eine ausführliche Dokumentation im Verzeichnis `/usr/share/doc/packages/` auf dem SuSE Firewall Adminhost. Außerdem gibt es zu jedem dieser Programme Man-Pages.

Erst wenn wirkliche alle Tests erfolgreich verlaufen sind, können Sie die Firewall in Betrieb nehmen. Bitte dokumentieren Sie alle von Ihnen durchgeführten Tests.

6.3 Inbetriebnahme

Um Ihre SuSE Linux Firewall in Betrieb zu nehmen, verbinden Sie zunächst nur das interne Netz mit der Firewall und stellen z. B. einen Laptop als externes Netz testweise bereit. Anschließend trennen Sie die Verbindung zum internen Netz und stellen die Verbindung zum Internet her. Testen Sie wenn möglich Ihre Firewall von extern. Kontrollieren Sie Ihr Setup.

6.3.1 Test von intern

Tests, die Sie durchführen sollten:

- Stehen alle Dienste zur Verfügung?
- Testen Sie von den internen Client-Rechnern aus, ob die Dienste funktionieren, die Sie zugelassen haben. Können Sie z. B. auf http/s zugreifen, E-Mails verschicken, per FTP Daten übertragen?
- Funktionieren Ihre Verbotsregeln?
- Testen Sie Ihren Paketfilter. Das können Sie mit einem Portscanner wie nmap machen. Verfolgen Sie die Log-Nachrichten auf dem Loghost oder Ihrer Firewall. Lassen Sie einen Paketsniffer mitlaufen, um verbotene Pakete aufzuspüren oder um zu sehen, ob Antwortpakete nicht ausgeliefert werden.
- Werden die Logdateien auf den Loghost geschrieben?

Fehlerbeseitigung:

Stellen Sie fest, was nicht funktioniert. Untersuchen Sie die Logfiles nach dem Prozessnamen, z. B. postfix oder named:

```
# grep postfix /var/log/messages
```

bzw.

```
# grep named /var/log/messages
```

Viele Programme kann man in den „Verbose-Modus“ schalten. Dadurch erhält man detailliertere Auskünfte (die zum Teil allerdings sehr umfangreich ausfallen können . . .).

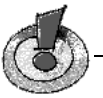
6.3.2 Test von extern

Testen Sie von extern, ob die freigeschalteten Dienste funktionieren. Verschicken Sie z. B. E-Mails nach intern. Sie sollten in `/var/log/mail` auf dem Firewall-Rechner die Meldungen von postfix sehen, ob die E-Mails angenommen wurden und an den internen Mailserver zugestellt werden konnten. Kontrollieren Sie, ob der Paketfilter funktioniert. Das können Sie mit einem Portscanner verifizieren. Gleichzeitig finden Sie die Meldungen des Kernel-Paketfilters in `/var/log/messages` bzw. in den Logverzeichnissen des Loghosts. Sie schlagen sich in "DENY"- und "ACCEPT"-Meldungen nieder. Versuchen Sie auch Verbindungen auf Ports aufzubauen, die Sie explizit verboten haben, und versuchen Sie, die korrespondierenden Log-Einträge zu finden und dem Ereignis zuzuordnen.

Wenn Sie einen Loghost verwenden, dann kontrollieren Sie, ob die Log-Meldungen vollständig übertragen werden.

6.3.3 „Echt“ ans Netz gehen

Erst wenn alle diese Tests erfolgreich abgeschlossen sind, verbinden Sie den Firewall-Rechner mit dem Internet und Ihrem Intranet und starten den Produktivbetrieb.



Hinweis

Kontrollieren Sie Ihre Log-Dateien ständig. Nur so können Sie rechtzeitig auf Angriffe oder Funktionsausfälle reagieren. Falls ungewöhnliche Ereignisse auftreten, reagieren Sie sofort. Erhöhen Sie Log-Level (falls möglich) und verfeinern Sie Ihre Log-Auswertung.

7 Hilfestellungen

In diesem Kapitel finden Sie Informationen, wie Sie ein Konzept für den Aufbau einer Firewall-Lösung mit der „SuSE Linux Firewall on CD“ für Ihr Netzwerk erstellen können. Sie haben auch jederzeit die Möglichkeit, die Dienstleistungen der SuSE Linux AG in Anspruch zu nehmen, um sich ein für Ihre Bedürfnisse maßgeschneidertes Konzept erarbeiten zu lassen.

7.1 Troubleshooting

Hier finden Sie Hilfestellungen, wenn sich der Adminhost nicht installieren lässt bzw. die SuSE Linux Live-CD for Firewall nicht bootet.

7.1.1 Probleme bei der Installation des Adminhosts

Wenn Sie Schwierigkeiten haben, den SuSE Linux Adminhost for Firewall zu installieren, steht Ihnen der kostenlose SuSE Linux Installationssupport zur Verfügung. Zuvor lohnt sich ein Blick in die Support-Datenbank. Hier finden sich zahlreiche Informationen zu diversen Installationsproblemen – eine Stichwortsuche hilft Ihnen dabei:

`http://sdb.suse.de`

7.1.2 Probleme beim Booten der Live-CD

Um die Fehlersuche zu vereinfachen, sollten Sie Folgendes beobachten und notieren:

- Was passiert beim Booten?
- Werden Dienste nicht gestartet, die konfiguriert wurden (skipped/failed Meldungen)?
- Gibt es Fehlermeldungen auf der Konsole?
- Gibt es auf dem tty9/tty12 Fehlermeldungen des Kernels? Um diese Meldungen zu sehen, wechseln Sie mit (Alt) + (F9) bzw. (Alt) + (F12) auf die entsprechende Konsole.

Probleme bei der Einbindung in das Netzwerk:

Beobachten und notieren Sie, welcher Art die Probleme sind. Testen Sie beispielsweise auf der Firewall (melden Sie sich als Benutzer `'root'` auf der Firewall an), ob die Netzwerk-Interfaces richtig konfiguriert sind:

```
root@firewall: # ifconfig
```

Dieser Befehl zeigt Ihnen, welche Interfaces konfiguriert sind und welche IP-Adressen, Netzwerkmasken usw. eingestellt sind. Falls notwendig korrigieren Sie die Konfiguration mit FAS und erstellen eine neue Konfigurationsdiskette. Damit die neue Konfiguration verwendet wird, muss der Rechner neu gestartet werden.

- Welche Dienste funktionieren von der Client-Seite (Intranet) aus? Sollen sie funktionieren? Anhand der Logfiles können Sie feststellen, ob es sich um unberechtigte Zugriffe handelt.

  Versuchen Sie Fehler zu reproduzieren.

- Funktionieren Zugriffe von außen auf freigegebene Ressourcen nicht? Welche Dienste sind betroffen? Soll die Ressource wirklich freigegeben sein?

  Testen Sie z. B. mit **ps**, ob der Prozess vorhanden ist, d. h. auch wirklich zur Verfügung steht. Wenn Dienste nicht zur Verfügung stehen, kontrollieren Sie Ihre Logfiles. Hier finden sich Meldungen, warum ein Dienst nicht gestartet wurde, oder ob versucht wurde, einen Dienst unberechtigterweise in Anspruch zu nehmen.

  Testen Sie von verschiedenen Clients, ob der Firewall-Rechner erreichbar ist und die Proxies ansprechbar sind.

7.2 Security-Policy und Kommunikationsanalyse

Für die sichere Anbindung eines internen Netzwerks an das Internet oder ein anderes „unsicheres“ Netzwerk sind im Vorfeld einige Dinge abzuklären. Dazu gehört die Erstellung der Security-Policy für das eigene Netzwerk und der Kommunikationsanalyse.

7.2.1 Die Security Policy

Die Security-Policy stellt die Grundlage für den Umgang mit allen Programmen, Rechnern und Daten dar. Weiterhin wird festgelegt, wie die Überwachung der Sicherheitsrichtlinien gewährleistet werden soll und wie Verstöße (von intern/extern) behandelt werden. Um eine Security-Policy zu erstellen, fertigt man am besten eine Kommunikationsanalyse an. Hierbei sind folgende Themen von großer Wichtigkeit:

- Zum einen gilt es, den Schutzbedarf zu analysieren. Was muss geschützt werden?

- Gibt es Bereiche im Intranet, die besonders schützenswerte Daten beinhalten (z. B. Personal-Abteilung, firmenkritische Daten etc.). Wo liegen diese Daten?
- Wer darf Zugriff auf die Daten haben? Gibt es abgestufte Zugangsberechtigungen?
- Sollen Daten via Netzwerk verfügbar sein?
- Welche Dienste sollen intern zur Verfügung stehen? Welche von intern nach extern (E-Mail, Surfen, Datentransfer) und welche von extern nach intern (E-Mail, Webdienste, Datentransfer)?

Die Liste der zu klärenden Fragen für eine Security-Policy muss individuell erstellt und beantwortet werden.

7.2.2 Kommunikationsanalyse

Die wichtigste Hilfestellung für die Durchführung einer Kommunikationsanalyse ist eine Kommunikations-Matrix.

Hier wird in Tabellenform dargestellt, welche Dienste für welchen Client-Rechner bzw. Benutzer zur Verfügung gestellt werden. Diese Matrix wird dann auf die Proxies/IP-Filter-Regeln abgebildet.

Erstellen einer Kommunikations-Matrix:

Fertigen Sie sich eine Liste aller Clients/Server Ihres Netzwerks an. Legen Sie dann fest, welche Protokolle von welchem Client verwendet werden dürfen. Definieren Sie außerdem, in welche Richtung die jeweiligen Pakete gesendet bzw. empfangen werden dürfen.

Ein Beispiel für das HTTP-Protokoll: Der Client host1 soll einen Webserver im internen Netz erreichen, aber keine Verbindung auf einen externen Webserver herstellen können. Der Eintrag in die Kommunikations-Matrix sieht dann für das HTTP-Protokoll wie im unten angeführten Beispiel aus.

Beispiel für eine Kommunikations-Matrix:

Protokoll	icmp		ftp		ssh		smtp		http		https		...
Client	intern	extern	i.	e.	i.	e.	i.	e.	i.	e.	i.	e.	
host1	x	–	x	–	–	–	x	–	x	–	–		
host2	x	–	–	–	x	–	x	–	–	–	–	–	
host3													
...													
hostn													

Anhand solch einer Kommunikations-Matrix behalten Sie immer den Überblick über die Kommunikationsbeziehungen innerhalb des Netzwerks. Das erleichtert Ihnen nicht nur die Konfiguration Ihres Netzwerks sondern auch gegebenenfalls die Fehleranalyse.

7.3 Dienstleistungen der SuSE Linux AG

Die SuSE Linux AG steht Ihnen gerne mit ihren Dienstleistungen zur Verfügung, bei:

- Beratung:
  Klärung des Schutzbedarfes, Kommunikationsanalyse
- Planung:
  - Hardwarebedarf
  - Netzwerkplanung/Integration
- Installation:
  - Vorortinstallation der Firewall-Lösung
  - Abnahme der Tests vor Ort/remote
  - Dokumentation
- Wartung:
  - Business-Support (kostenpflichtig)
  - Online-Wartung via Modem/Callback (durch das Consulting/Business-Support)

7.4 Updates

Beim Betrieb einer Firewall ist die permanente Pflege der eingesetzten Software enorm wichtig. Sobald eine Sicherheitslücke entdeckt und behoben ist, muss ein Update der entsprechenden Software stattfinden.

Falls ein solches Sicherheitsupdate die SSuSE Linux Live-CD for Firewall"betrifft, wird eine neue Live-CD an Sie verschickt. Diese Update-CD legen Sie einfach in das CD-Laufwerk des Firewall-Rechners ein und starten die Firewall neu.

Sicherheitsrelevante Updates für den SuSE Linux Adminhost for Firewall werden auf dem SuSE FTP-Server zur Verfügung gestellt. Diese Pakete laden Sie auf den Adminhost und installieren sie z. B. mit dem Kommando

```
root@adminhost:# rpm -Uhv neuespaket.rpm
```

Verfolgen Sie bitte auch die Hinweise, die auf den Security-Mailinglisten und dem SuSE Webserver veröffentlicht werden:

`http://lists2.suse.com/archive/suse-security`

`http://www.suse.de/de/support/security/index.html`

7.5 Maßnahmen im Falle eines Einbruchs

7.5.1 System-Einbruch und Ereignisanzeige

Ein „richtig“ konfiguriertes Linux/UNIX-System kann an sich schon als ziemlich sicher gelten. Systemimmanente Gefahren, die mit einem komplexen System wie Linux bzw. UNIX zusammenhängen, werden besser erkannt als bei anderen Betriebssystemen, weil UNIX seit mehr als 30 Jahren eingesetzt und weiterentwickelt wird. UNIX ist die Grundlage des Internets. Nichtsdestotrotz werden Konfigurationsfehler gemacht und tauchen immer wieder Sicherheitslücken auf. Es wird immer Sicherheitsmängel geben. Sicherheitsexperten und Cracker/Hacker stehen im immerwährenden „Konkurrenzkampf“, einander immer einen Schritt voraus zu sein. Was heute noch als sicher gilt, kann morgen schon wieder unsicher sein.

Anzeichen für einen Einbruch in Ihr System (engl. *Intrusion Detection*)

Als Anzeichen für eine Kompromittierung Ihres Systems können Sie alles betrachten, was vom „normalen“ Verhalten Ihres Firewall-Systems abweicht, z. B.:

- erhöhte Prozessorlast,
- außergewöhnlich großer Netzwerkverkehr,
- ungewöhnliche Prozesse oder
- Prozesse werden von Benutzern gestartet, die nicht existierten.

Einen Angriff erkennen

Zunächst sollte man sich im Klaren darüber werden, welche Art von Aktionen als Angriff zu bewerten sind. Leider ist es in der Zwischenzeit vollkommen normal, dass ein Rechner, der mit dem Internet verbunden ist, nach offenen, verwundbaren Ports abgescannt wird. Ebenso ist es üblich, Ports anzugreifen, die irgendwann als verwundbar bekannt geworden sind (pop3/qpopper, rpc-mountd, smtp/sendmail). Die meisten dieser „Angriffe“ werden von „Skript-Kiddies“ durchgeführt. Verwendet werden vorgefertigte „Exploits“, die auf einschlägigen Web-Seiten veröffentlicht werden (z. B. `http://www.rootshell.com`). Diese Seiten stellen aber auch eine wertvolle Informationsquelle für Netzwerk- und Systemadministratoren dar. Sie sind meistens daran zu erkennen, dass der Angriff nur ein einziges Mal durchgeführt und bei Misserfolg nicht wiederholt wird. Als erste Maßnahme auf solch ein Vorkommnis sollten Sie überprüfen, ob wirklich ein Einbruch stattgefunden hat. Des Weiteren sollten Sie die Log-Level erhöhen und die Auswertung verfeinern (z. B. gezielt nach einer angreifenden IP-Adresse in den Log-Files oder nach ungewöhnlichen Port-Nummern suchen).

Es bleibt Ihnen überlassen, was Sie als gefährlichen Angriff auf Ihr System betrachten. Aber legen Sie unbedingt eine Vorgehensweise fest, wie Sie auf ein solches Ereignis reagieren.

Was ist zu tun, wenn Sie einen Angriff vermuten? Hierzu ist folgende Literatur zu empfehlen:

„Steps for Recovering from a Unix Root Compromise“ (`http://www.cert.org/tech_tips/root_compromise.html`)

RFC 2196: Site Security Handbook

Diese beiden Veröffentlichungen beschreiben Maßnahmen, die auf einen erfolgreichen Einbruch folgen sollten. Die Dokumente liefern einen formalen Ansatz, wie eine Firma, Behörde oder Bildungseinrichtung reagieren kann. Das dort diskutierte Vorgehen setzt eine gewisse Menge an Speicherplatz voraus, um „Snapshots“ des Systems anfertigen zu können, zudem Mitarbeiter für die Analyse und Beurteilung des Sicherheitsproblems und es sind Situationen beschrieben, in denen es angebracht erscheint, Strafverfolgungs-Maßnahmen zu ergreifen.

Was ist zu tun, wenn Sie einen erfolgreichen Angriff vermuten:

- Es ist wichtig, dass Sie Ruhe bewahren. Unbedachte Handlungen können wichtige Informationen zerstören (z. B. Prozesse, die von einem Eindringling gestartet wurden).
- In der Security-Policy sollte festgelegt sein, was zu tun und wer zu informieren ist. Die Kommunikation sollte dann aber nicht per E-Mail, sondern via Telefon oder Fax erfolgen.
- Trennen Sie die Netzwerkverbindungen zur Firewall physikalisch. Es ist keine gute Idee, den Rechner herunterzufahren. Wichtige Informationen könnten verloren gehen, z. B. Programme, die vom Eindringling per Hand gestartet wurden.
- Listen Sie sich alle laufenden Prozesse mit ps auf und suchen Sie nach Prozessen, die im Normalbetrieb der Firewall nicht auftreten.
- Erstellen Sie sich eine Prozesstabelle bei der Inbetriebnahme der Firewall, die Sie dann als Vergleichsgrundlage verwenden können.
- Untersuchen Sie die laufenden Prozesse nach Bindungen an ungewöhnliche TCP- oder UDP-Ports.
- Wurden die Paketfilter-Regeln verändert?
- Vergleichen Sie alle Konfigurationsdateien mit der originalen Konfiguration. Das ist bei der „SuSE Linux Firewall on CD“ sehr einfach. Die Konfiguration ist ja auf dem Adminhost gespeichert. Hierfür ist es jedoch wichtig, dass Sie den Firewall-Rechner nicht neu starten, weil sonst Änderungen an den Filterregeln verloren gehen!
- Sichern Sie außerdem alle Logfiles. Die Logfiles können strafrechtlich relevante Beweismittel sein. Dokumentieren Sie alle Schritte, die Sie unternommen haben. Wenn Sie die Logfiles lokal auf die Festplatte speichern, sollten Sie eine 1:1-Kopie der Festplatte für Dokumentationszwecke anfertigen.
- Sichern Sie Ihre Daten auf CD oder einem anderen Medium (Bandlaufwerk, ZIP-Drive).

- Werten Sie die Logfiles aus: Wer versuchte wann und von wo aus (IP-Adresse, Domainname, eventuell sogar Benutzername) auf welche Dienste/Ports zuzugreifen? Wurde versucht, Passwörter zu erraten (mehrfach fehlgeschlagene Login-Versuche mit ein und derselben Benutzerkennung)?
- Sorgen Sie unbedingt dafür, dass Sie für alle Ihre Rechner/Server eine einheitliche, genaue Zeitquelle verwenden. Es ist wichtig, dass die Rechneruhren des Firewall-Rechners und des Log-Hosts möglichst exakt übereinstimmen. Wenn möglich, verwenden Sie eine gemeinsame Zeitquelle für alle Ihre Server. Nur so sind Ereignisse auf verschiedenen Rechnern exakt zuzuordnen.
- Welche Teile der Security-Policy wurden verletzt? Dies ist vor allem bei internen Angriffen von Bedeutung.
- Deaktivieren Sie eventuell den Benutzer-Account in Ihrem Netzwerk, der den Angriff durchgeführt hat. Das jeweilige Vorgehen bei internen Verstößen sollte auch geregelt sein (Security- bzw. Firmenpolitik).

7.5.2 Angriffe von außen

Informieren Sie den für den Adress-Block zuständigen Systemadministrator (via Postmaster- bzw. Abuse-Adresse der Domain).

Es stellt sich die Frage, welche Informationen Sie weitergeben sollten. Der Bericht über einen Zwischenfall oder Angriff sollte genug Informationen enthalten, um es der anderen Seite zu ermöglichen, das Problem zu ermitteln. Denken Sie jedoch daran, dass Ihre Kontaktperson derjenige sein könnte, der Sie angegriffen hat. Hier ist eine Liste der möglichen Angaben, die Sie weitergeben können. Wählen Sie aus, was Sie weitergeben wollen:

- Ihre E-Mail-Adresse,
- Telefonnummer,
- Ihre IP-Adresse, Hostname, Domainname,
- die IP-Adressen, Hostnamen, Dommainnamen, die an dem Angriff beteiligt waren,
- das Datum und die Uhrzeit des Angriffs, am besten mit Zeitzone relativ zur GMT,
- eine Beschreibung des Angriffs,
- wie der Angriff bemerkt wurde,
- Auszüge aus den Logfiles, die sich auf den Angriff beziehen,
- eine Beschreibung des Logfile-Formats,
- Angabe von Advisories und Security-Informationen, welche die Art und Schwere des Angriffs beschreiben,

- was Sie von der angesprochenen Person fordern, z. B. das Schließen eines Accounts, Bestätigung des Angriffs, eine Erklärung, eine Information, Bitte um weitere Beobachtung.

Wenn Sie alle Maßnahmen zur Datensicherung und Dokumentation durchgeführt haben, nehmen Sie Ihre Firewall wieder in Betrieb. Soweit möglich, erhöhen Sie die Loglevel der einzelnen Programme. Es ist ziemlich sicher, dass der Angreifer erneut versucht, in Ihr System einzudringen. Das ist dann der Moment, in dem Sie die Möglichkeit haben, den Angreifer dingfest zu machen.

Beispiele:

Melden Sie sich auf der Konsole an.

Untersuchen Sie die Logfiles.

Zum Beispiel:

```
# grep DENY /var/log/messages | less
```

Mit diesem Befehl sehen Sie alle Zeilen, die ein `DENY` enthalten, die also vom Paketfilter des Kernels aufgezeichnet worden sind. Sie können jetzt z. B. nach bestimmten auffällig gewordenen IP-Adressen suchen (gehäuftes Auftreten von DENY-Meldungen von IP-Adressen, auf eine oder mehrere Port-Nummern). Finden Sie heraus, was genau passiert ist. Mit den schon beschriebenen Werkzeugen lassen sich die Logfiles nach definierbaren Kriterien durchsuchen. Problem: Manchmal weiß man nicht, was man sucht, bis man es findet … Es kann auch sein, dass sich ein Systemadministrator eines anderen Netzwerks bei Ihnen via Postmaster- bzw. Abuse-Mailadresse meldet und sich beschwert, dass von Ihrem Netz aus Angriffe auf fremde Rechner stattgefunden haben. Nehmen Sie diese Beschwerden ernst. Lassen Sie sich auf alle Fälle Protokolle über die Angriffe zusenden, damit Sie Anhaltspunkte zu Datum und Uhrzeit haben und mit welchen Mitteln das fremde System angegriffen wurde. Versuchen Sie, die Tatbestände zu verifizieren. Es kann sein, dass ein Hacker, Cracker oder Angreifer bereits Ihre Sicherheitsschranken überwunden hat und Ihr Netzwerk für seine Zwecke missbraucht. Auch hier steht der Ruf Ihres Unternehmens auf dem Spiel.

Wenn Sie alles gesichert und dokumentiert haben, überprüfen Sie Ihre Firewall-Konfiguration. Nach Beheben von eventuellen Fehlern oder Abschalten von Diensten, die Sie für gefährdet halten, starten Sie Ihre Firewall neu. Hier zeigt sich ein klarer Vorteil der „SuSE Linux Firewall on CD“, denn durch einfaches Booten des Firewall-Rechners wird der ursprüngliche Zustand wieder hergestellt, eine aufwendige Neuinstallation des Betriebssystems und das Einspielen von Backups entfällt.

7.5.3 Vorteil des Live-Filesystems der „SuSE Linux Firewall on CD“

Einer der größten Vorteile der SuSE Firewall ist, dass sie durch einfaches Booten wieder in den Ausgangszustand zu versetzen ist. Allerdings ist dabei natürlich zu beachten, dass auch eventuelle Konfigurationsfehler wieder vorhanden sind.

Sollte der Fall eingetreten sein, dass die Firewall überwunden worden ist, muss herausgefunden werden, wie der Einbruch stattgefunden hat, um die fehlerhafte Konfiguration korrigieren zu können. Falls Programme Sicherheitslücken aufweisen, stellt die SuSE Linux AG Updates für die betroffenen Programme zur Verfügung – das heißt im Falle der „SuSE Linux Live-CD for Firewall“ eine neue CD.

Hier können Sie weitere Informationen finden:

`http://www.cert.org` und

`http://www.first.org`

7.6 Professionelle Hilfe und Support

Wenn Sie einen Angriff vermuten, sich aber trotz der oben beschriebenen Maßnahmen zur Überprüfung nicht sicher sind, ob es wirklich zu einer Kompromittierung Ihres Netzes gekommen ist, leiten Sie unbedingt erste Sicherheitsmaßnahmen ein. Das bedeutet vor allem die Netzwerkverbindungen physikalisch zu trennen.

Wenden Sie sich mit Ihren Fragen an den Händler bei dem Sie die SuSE Firewall on CD erworben haben oder an SuSE. In diesen Fällen können Sie auch immer die Dienstleistungen der SuSE Linux AG in Anspruch nehmen.

7.6.1 Supportbestimmungen

Umfang des Installationssupports

Der Installationssupport soll Ihnen helfen, Ihr SuSE Linux System einsatzfähig zu installieren. Dies gilt für die zentralen Komponenten des Systems, die einen prinzipiellen Betrieb ermöglichen. Dazu zählen:

- Die Installation des SuSE Linux-Grundsystems von der „Admin-CD for Firewall“ auf einem Rechner bis zum erfolgreichen Start des „Firewall Administration Systems“ (FAS).
- Die Konfiguration der Basis-Hardware dieses Rechners mit dem graphischen Installationstool YaST2, d. h. der PC-Zentralkomponenten, ohne Peripheriegeräte, jedoch inklusive der Einrichtung einer Ethernetkarte.

Alle hier nicht genannten Themen werden im Rahmen des Installationssupports nicht behandelt.

Zeitraum des Installationssupports

Der Installationssupport für die Admin-CD for Firewall erstreckt sich über einen Zeitraum von 30 Tagen ab dem Registrierdatum.

Wie erreichen Sie das SuSE Support Team?

Sie können unser Support-Team per E-Mail, Fax oder Brief erreichen:

- **per E-Mail:**
  Adresse: fw-support@suse.de
  Bearbeitung: wochentags
- **per Fax:**
  Faxnummer: (09 11) 74 05 34 77
  Bearbeitung: wochentags
- **per Brief:**
  Anschrift: SuSE GmbH
  – Support –
  Schanzäckerstr. 10
  D-90443 Nürnberg
  Bearbeitung: wochentags

7.6.2 Kostenpflichtiger Support

Selbst wenn ein Betriebssystem alle Anlagen dazu mitbringt: Erst durch professionelle und kompetente Betreuung wird es zur ernsthaften Alternative für den Einsatz im betrieblichen Alltag. SuSE garantiert diesen Service für Linux. Alle Informationen hierzu finden Sie ebenfalls beim zentralen Support-Portal für SuSE Linux:

http://support.suse.de

Individuelle Projekte und Beratung

Sie möchten SuSE Linux in Ihrem Unternehmen einsetzen. Wir bieten Ihnen kompetente Beratung und Lösungen, um Linux auch in Ihrem IT-Umfeld optimal nutzen zu können.

Wir haben als kompetenter Linux-Anbieter viel Erfahrung im Einsatz von Linux-Servern gewonnen. Nutzen Sie das Know-how unser Experten, um Ihre Projekte erfolgreich durchzuführen. Unsere Stärke ist unsere Vielseitigkeit, ob es um Datenbanken, Security-Konzepte, Internet-Anbindung oder firmenweite Vernetzung geht: Linux ist mit der richtigen Software eine starke Plattform für Ihre Anwendungen.

Unser Angebot reicht von der Konzeption, Implementation und Konfiguration von Server-Systemen bis zur kompletten Infrastruktur-Beratung.

Sie möchten z. B. Ihre Internet-Präsenz auf Basis von SuSE Linux realisieren und benötigen eine entsprechende Lösung für Web-Server, E-Mail und sichere Internet-Anbindung? Unsere Systemberater konzipieren und implementieren mit Ihnen gemeinsam die richtige Lösung.

Sie betreuen ein komplexes, heterogenes Netzwerk und möchten Linux integrieren? Wir beraten und unterstützen Sie bei Design und Rollout komplexer Server-Lösungen.

Sie haben spezielle Anforderungen, die mit Standard-Software nicht abzudecken sind? Wir können Ihnen mit individuellen Entwicklungen weiterhelfen:

SuSE Linux AG
Schanzäckerstraße 10
D-90443 Nürnberg
Tel: +49-911-740-53-0
Fax: +49-911-740-53-479
E-Mail: suse@suse.de

Vertreten durch unsere Regional Service Center im In- und Ausland, ebenso wie durch unser Support- und Development-Center in Nürnberg. Dabei unterstützt Sie vor Ort die *SuSE Linux AG*:

- Rollout- und Implementation-Services
- Infrastruktur-Beratung
- Intranet-Server-Lösungen
- Internet-Server-Lösungen
- Entwicklung kundenspezifischer Anpassungen
- Komplettlösungen
- E-Commerce

7.6.3 SuSE-Trainingsprogramm

SuSE bietet Ihnen Trainings und Workshops rund um Linux an. Unser umfassendes Programm reicht von Einsteigerkursen über Administrationsschulungen bis hin zu Trainings für Entwickler und Vorbereitungskursen zur LPI-Zertifizierung. Nur SuSE Trainer bzw. von SuSE Training zertifizierte Trainer (SCLT), die unseren hohen Ansprüchen genügen, halten unsere Schulungen und sorgen damit für höchstes Niveau. Um einen hohen Wissenstransfer zu garantieren, legen wir Wert auf aktuelle, didaktisch optimal aufbereitete und praxisbezogene Inhalte.

Mit dem SuSE-Trainingsprogramm können Sie das Wissen aufbauen und vertiefen, das ein erfolgreiches Unternehmen im IT-Bereich benötigt. Buchen Sie einen Kurs in den SuSE-eigenen Schulungszentren oder bei einem unserer zertifizierten Schulungsspartner in Ihrer Nähe. Eigene Schulungszentren unterhalten wir in München und Dortmund. Unsere Trainer kommen auch gerne zu Ihnen, um Ihre Mitarbeiter individuell und auf Ihre Bedürfnisse zugeschnitten zu schulen. Eine stets aktuelle Übersicht aller Termine sowie eine detaillierte Beschreibung der Kursinhalte finden Sie unter:

http://www.suse.de/de/support/training

7.6.4 Feedback

Wir sind Ihnen immer für Hinweise und Problembeschreibungen dankbar und helfen auch gerne weiter, wenn das Problem grundlegender Natur ist oder wir bereits eine Lösung dafür haben.

Wir sind immer bemüht, ein SuSE Linux-System aufzubauen, das den Wünschen unser Kunden möglichst nahe kommt. Deshalb haben wir für Kritik an der CD und am Buch, sowie für Anregungen zu künftigen Projekten, immer ein offenes Ohr. Wir denken, dies ist der beste Weg, Fehlentwicklungen frühzeitig zu erkennen und den hohen Qualitätsstandard von Linux zu erhalten.

Sie können uns Ihr Feedback jederzeit via E-Mail an feedback@suse.de schreiben.

7.6.5 Weitere Dienstleistungen

Ferner möchten wir auf die folgenden, kostenlosen Dienstleistungen hinweisen, die Ihnen rund um die Uhr zur Verfügung stehen:

- **SuSE WWW-Server**

  `http://www.suse.de`

  Aktuelle Informationen, Kataloge, Bestellservice, Support-Formular, Support-Datenbank

- **SuSE Mailing-Listen** (Informationen und Diskussionsrunden via E-Mail):
  - suse-announce@suse.com – Ankündigungen und Infos der SuSE GmbH (deutsch)
  - suse-announce-e@suse.com – Ankündigungen und Infos der SuSE GmbH (englisch)
  - suse-linux@suse.com – Diskussionen rund um die SuSE Linux-Distribution (deutsch)
  - suse-linux-e@suse.com – Diskussionen rund um SuSE Linux (englisch)
  - proxy-suite@suse.com – Diskussion über die SuSE Proxy-Suite (englisch)
  - suse-adabas@suse.com – Infos zu und Diskussion über Adabas-D unter SuSE Linux (deutsch)
  - suse-applix@suse.com – Erfahrungsaustausch zum **Applixware**-Paket der SuSE GmbH (deutsch)
  - suse-axp@suse.com – SuSE Linux auf Alpha-Prozessoren (englisch)
  - suse-domino@suse.com – Informationen und Diskussion zu SuSE Linux und Lotus Domino (deutsch)
  - suse-ham@suse.com – SuSE Linux und Amateurfunk (deutsch)
  - suse-ham-e@suse.com – SuSE Linux und Amateurfunk (englisch)
  - suse-ibm-db2@suse.com – SuSE Linux und IBM DB2 (englisch)

- suse-isdn@suse.com – ISDN mit SuSE Linux (deutsch)
- suse-informix@suse.com – Infos zu und Diskussion über Informix unter SuSE Linux (englisch)
- suse-laptop@suse.com – SuSE Linux auf Laptops (deutsch)
- suse-motif@suse.com – SuSE Linux und Motif (englisch)
- suse-oracle@suse.com – Infos zu und Diskussion über Oracle unter SuSE Linux (englisch)
- suse-ppc@suse.com – SuSE Linux auf Power-PC-Prozessoren (englisch)
- suse-security@suse.com – Diskussion zu Sicherheitsbelangen unter SuSE Linux (englisch)
- suse-security-announce@suse.com – Ankündigung von sicherheitsrelevanten Fehlern und Updates (englisch)
- suse-sparc@suse.com – SuSE Linux auf Sparc-Prozessoren (englisch)

Um sich bei einer Liste einzutragen, schicken Sie eine E-Mail-Nachricht an:

<LISTNAME>`-subscribe@suse.com`

Es wird eine automatische Rückfrage kommen, die Sie bitte bestätigen müssen.

Anstelle von <LISTNAME> ist der Name der jeweils gewünschten Mailing-Liste einzusetzen; z. B. suse-announce-subscribe@suse.com, um die regelmäßigen Ankündigungen zu erhalten.

Ähnlich ist das Vorgehen, wenn Sie eine Liste abbestellen wollen:

<LISTNAME>`-unsubscribe@suse.com`

Achten Sie bitte darauf, dass die **`unsubscribe`**-Mail mit Ihrer korrekten E-Mail-Adresse geschickt wird.

- **SuSE FTP-Server**

  `ftp://ftp.suse.com`

  aktuelle Information, Updates und Bugfixes

  Melden Sie sich bitte beim System als Benutzer `'ftp'` an.

7.7 Literaturhinweise

- D. Brent Chapman & Elizabeth D. Zwicky: *Einrichten von Internet-Firewalls*, O'Reilly 2000.
- Wolfgang Barth: *SuSE Firewall Buch*, SuSE Press 2001.
- *Maximum Linux Security*, SAMS 1999.
- Robert L. Ziegler: *Linux Firewalls*, New Riders 1999.

A DNS – Domain Name Service

DNS (engl. *Domain Name Service*) wird benötigt, um die Domain- und Rechnernamen in IP-Adressen aufzulösen.

A.1 Nameserver BIND starten

Der Nameserver BIND8, das gilt auch für die neue Version BIND9, ist auf SuSE Linux bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann.

Hat man bereits eine funktionsfähige Internetverbindung und trägt in der `/etc/resolv.conf` als Nameserver 127.0.0.1 für localhost ein, hat man in der Regel schon eine funktionierende Namensauflösung, ohne dass man den DNS des Providers kennt. BIND führt so die Namensauflösung über die Root-Nameserver durch, was aber merklich langsamer ist. Normalerweise sollte man den DNS des Providers mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter **`forwarders`** eintragen, um eine effektive und sichere Namensauflösung zu erhalten. Funktioniert das soweit, läuft der Nameserver als reiner „Caching-only“-Nameserver. Erst wenn man ihm eigene Zonen bereitstellt, wird er ein richtiger DNS werden. Ein einfaches Beispiel dafür, findet man im Doku-Verzeichnis: `/usr/share/doc/packages/bind8/sample-config`.

Man sollte allerdings keine offizielle Domain aufsetzen, solange man diese nicht von der zuständigen Institution – für '.de' ist das die DENIC eG – zugewiesen bekommen hat. Auch wenn man eine eigene Domain hat, diese aber vom Provider verwaltet wird, sollte man diese besser nicht verwenden, da BIND sonst keine Anfragen für diese Domain mehr forwarden würde und so z. B. der Webserver beim Provider für die eigene Domain nicht mehr erreichbar wäre.

Um den Nameserver zu starten gibt man auf der Kommandozeile (als root)

```
rcnamed start
```

ein. Erscheint rechts in grün „done“, ist der `named`, so heißt der Nameserver-Prozess, erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit des Nameservers sofort testen, indem man das Programm `nslookup` verwendet. Als Default Server muss localhost mit der Adresse 127.0.0.1 angezeigt werden. Sollte das nicht der Fall sein, steht wahrscheinlich in der `/etc/resolv.conf` ein falscher Nameserver oder diese Datei existiert gar nicht. Für einen ersten Test gibt man auf dem Prompt von `nslookup` „127.0.0.1“ ein, das sollte immer funktionieren; erhält man stattdessen eine Fehlermeldung „No response from server“ oder ähnlich, dann sollte man mit folgendem Kommando überprüfen, ob der `named` überhaupt läuft

```
rcnamed status
```

Falls der Nameserver nicht startet oder ein fehlerhaftes Verhalten zeigt, findet man die Ursache in den meisten Fällen in „/var/log/messages“ protokolliert.

Hat man eine Wählverbindung, muss man beachten, dass BIND8 beim Starten die Root-Nameserver überprüfen will. Gelingt ihm das nicht, weil keine Internetverbindung zustande kommt, kann das dazu führen, dass überhaupt keine DNS-Anfragen außer für lokal definierte Zonen aufgelöst werden können. BIND9 verhält sich da anders, benötigt aber ein Mehrfaches an Ressourcen im Vergleich zu BIND8.

Um den Nameserver des Providers, oder einen eigenen, den man schon im eigenen Netz laufen hat, als „forwarder“ zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt **`options`** unter **`forwarders`** ein; vgl. Beispiel A.1.1.

```
options {
          directory "/var/named";
          forwarders { 10.11.12.13; 10.11.12.14; };
          listen-on { 127.0.0.1; 192.168.0.99; };
          allow-query { 127/8; 192.168.0/24; };
          notify no;
        };
```

Datei A.1.1: Forwarding-Optionen in `named.conf`

Die im Beispiel verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten eingetragen werden.

Nach den **`options`** folgen dann die Einträge für die Zonen, die Einträge für „localhost“, „0.0.127.in-addr.arpa“, sowie „.“ vom „type hint“ sollten mindestens immer vorhanden sein. Die zugehörigen Dateien müssen nicht verändert werden, da sie so funktionieren wie sie sind. Beachten muss man auch, dass nach jedem Eintrag ein „;“ steht und die geschweiften Klammern korrekt gesetzt sind. Hat man nun Änderungen an der Konfigurationsdatei `/etc/named.conf` oder an den Zonen-Dateien vorgenommen, muss man BIND dazu bringen diese neu einzulesen. Das gelingt mit dem Kommando **`rcnamed reload`**. Alternativ kann man den Nameserver auch komplett neu starten, durch den Befehl **`rcnamed restart`**. Fehlt nur noch das Kommando, um den Nameserver wieder zu beenden: **`rcnamed stop`**. Soll der `named` bereits beim Booten gestartet werden, muss man in `/etc/rc.config` lediglich den Eintrag **`START_NAMED=no`** auf **`START_NAMED=yes`** abändern.

A.2 Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen zum Nameserver BIND8 bzw. BIND9 sind in der Datei `/etc/named.conf` vorzunehmen. Die Zonendaten selbst, die Rechnernamen, IP-Adressen usw. für die zu verwaltenden Domains, sind in separaten Dateien im Verzeichnis `/var/named` abzulegen, dazu aber unten mehr.

Die `/etc/named.conf` unterteilt sich grob in zwei Bereiche, zum einen der Abschnitt **`options`** für allgemeine Einstellungen und zum anderen die **`zone`**-Einträge für die einzelnen Domains. Außerdem kann man noch einen Bereich

logging, sowie Einträge vom Typ **acl** definieren. Kommentarzeilen beginnen mit einem '#'-Zeichen, alternativ ist '///' auch erlaubt.

Eine minimalistische /etc/named.conf stellt Beispiel A.2.1 dar.

```
options {
        directory "/var/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Datei A.2.1: Minimalistische Datei /etc/named.conf

Dieses Beispiel funktioniert für Bind8 und Bind9 gleichermaßen, da keine speziellen Optionen verwendet werden, die nur von einer Version verstanden werden. Bind-9.1.1 akzeptiert alle Bind8-Konfigurationen und vermerkt allenfalls beim Start, wenn eine Option nicht implementiert ist. Spezielle Bind9-Optionen werden vom Bind8 aber nicht unterstützt.

A.2.1 Die wichtigsten Konfigurationsoptionen im Abschnitt options

directory "/var/named"; gibt das Verzeichnis an, in dem der BIND die Dateien mit den Zonendaten findet,

forwarders { 10.0.0.1; }; verwendet man, um den oder die Nameserver (meist des Providers) anzugeben, an den oder die DNS-Anfragen weitergereicht werden, die nicht direkt beantwortet werden können.

forward first; bewirkt, dass die DNS-Anfragen zu erst geforwarded werden, bevor versucht wird diese über die Root-Nameserver aufzulösen. Anstelle von **forward first** kann man auch **forward only** schreiben, dann werden alle Anfragen weitergeleitet und die Root-Nameserver werden gar nicht mehr angesprochen. Das kann für Firewall-Konfigurationen sinnvoll sein.

listen-on port 53 { 127.0.0.1; 192.168.0.1; }; sagt dem BIND, auf welchen Netzwerkinterfaces und welchem Port er auf Anfragen der Clients horcht. Die Angabe **`port 53`** kann man sich dabei sparen, da 53 ohnehin der Standardport ist. Lässt man diesen Eintrag komplett weg, werden standardmäßig alle Interfaces verwendet

query-source address * port 53; Dieser Eintrag kann notwendig sein, wenn eine Firewall die externen DNS-Abfragen blockiert. So wird BIND dazu gebracht, Anfragen nach außen von Port 53 aus und nicht von den hohen Port's > 1024 zu stellen.

allow-query { 127.0.0.1; 192.168.1/24; }; bestimmt die Netze aus denen Clients DNS-Anfragen stellen dürfen. Das **`/24`** ist dabei eine Kurzschreibweise für die Netzmaske, in diesem Fall 255.255.255.0.

allow-transfer { ! *; }; regelt welche Rechner Zonentransfers anfordern dürfen, dieses Beispiel unterbindet sie, aufgrund des **`!`** **`*`** komplett. Ohne diesen Eintrag können Zonentransfers ohne Einschränkungen von überall angefordert werden.

statistics-interval 0; Ohne diesen Eintrag produziert Bind8 stündlich mehrere Zeilen Statisikmeldungen in `/var/log/messages`. Die Angabe von 0 bewirkt, dass diese komplett unterdrückt werden, ansonsten kann man hier die Zeit in Minuten angeben.

cleaning-interval 720; Diese Option legt fest, in welchem Zeitabstand Bind8 seinen Cache aufräumt. Die Aktivität führt jedes Mal zu einem Eintrag in /var/log/messages. Die Zeitangabe erfolgt in Minuten. Voreingestellt sind 60 Minuten.

interface-interval 0; Bind8 durchsucht regelmäßig die Netzwerkschnittstellen nach neuen oder nicht mehr vorhandenen Interfaces. Setzt man diesen Wert auf **`0`**, so wird darauf verzichtet und Bind8 lauscht nur auf den beim Start gefundenen Interfaces. Alternativ kann man das Intervall in Minuten angeben. Voreingestellt sind 60 Minuten.

notify no; Das **`no`** bewirkt, dass keine anderen Nameserver benachrichtigt werden, wenn an den Zonendaten Änderungen vorgenommen werden oder der Nameserver neu gestartet wird.

A.2.2 Der Konfigurationsabschnitt „Logging“

Was und wie wohin mitprotokolliert wird, kann man beim Bind8 recht vielseitig konfigurieren. Normalerweise sollte man mit den Voreinstellungen zufrieden sein können. Beispiel A.2.2 auf der nächsten Seite zeigt die einfachste Form so eines Eintrages und unterdrückt das „Logging“ komplett

A.2.3 Aufbau der Zonen-Einträge

Nach **`zone`** wird der Name der zu verwaltenden Domain angegeben, hier willkürlich **`meine-domain.de`** gefolgt von einem **`in`** und einem in geschweiften

```
logging {

        category default { null; };

};
```

Datei A.2.2: Logging wird unterdrückt

```
zone "meine-domain.de" in {
        type master;
        file "meine-domain.zone";
        notify no;
};
```

Datei A.2.3: Zone-Eintrag für meine-domain.de

Klammern gesetzten Block zugehöriger Optionen; vgl. Beispiel A.2.3. Will man eine „Slave-Zone“ definieren, ändert sich nur der **`type`** auf **`slave`** und es muss ein Nameserver angegeben werden, der diese Zone als **`master`** verwaltet (kann aber auch ein „slave“ sein); vgl. Beispiel A.2.4.

```
zone "andere-domain.de" in {
        type slave;
        file "slave/andere-domain.zone";
        masters { 10.0.0.1; };
};
```

Datei A.2.4: Zone-Eintrag für andere-domain.de

Die Optionen:

type master; Das **`master`** legt fest, dass diese Zone auf diesem Nameserver verwaltet wird. Das setzt eine sauber erstellte Zonendatei voraus.

type slave; Diese Zone wird von einem anderen Nameserver transferiert. Muss zusammen mit **`masters`** verwendet werden.

type hint; Die Zone `.` vom Typ **`hint`** wird für die Angabe der Root-Nameserver verwendet. Diese Zonendefinition kann man unverändert lassen.

file „meine-domain.zone“ oder file „slave/andere-domain.zone“; Dieser Eintrag gibt die Datei an, in der die Zonendaten für die Domain eingetragen sind. Bei einem **`slave`** braucht die Datei nicht zu existieren, da ihr Inhalt von einem anderen Nameserver geholt wird. Um Master- und Slave-Dateien auseinander zu halten, gibt man für die Slave-Dateien das Verzeichnis `slave` an.

masters { 10.0.0.1; }; Diesen Eintrag braucht man nur für Slave-Zonen und er gibt an, von welchem Nameserver die Zonendatei transferiert werden soll.

allow-update { ! *; }; diese Option regelt den Schreibzugriff von extern auf die Zonendaten. Damit wäre es Clients möglich, sich selbst im DNS einzutragen, was aus Sicherheitsgründen nicht wünschenswert ist. Ohne diesen Eintag, sind Zonen-Updates generell untersagt, dieses Beispiel würde daran auch nichts ändern, da **!** ***** ebenfalls alles verbietet.

A.2.4 Aufbau der Zonendateien

Man benötigt zwei Arten von Zonen-Dateien, die einen dienen dazu, einem Rechnernamen die IP-Adresse zu zuordnen und die anderen gehen den umgekehrten Weg und liefern zu einer gegebenen IP-Adresse den Rechnernamen.

Eine wichtige Bedeutung hat der '.' in den Zonendateien. Werden Rechnernamen, ohne abschließenden '.' angegeben, wird immer die Zone ergänzt. Man muss also komplette Rechnernamen, die bereits mit vollständiger Domain angegeben wurden, mit einem '.' abschließen, damit die Domain nicht noch einmal dran gehängt wird. Ein fehlender Punkt oder einer an der falschen Stelle, dürfte die häufigste Fehlerursache bei der Konfiguration von Nameservern sein.

Den ersten Fall betrachten wir an der Zonen-Datei `welt.zone`, die für die Domain `welt.all` zuständig ist;vgl. Datei A.2.5.

```
1.  $TTL 2D
2.  welt.all.   IN SOA      gateway  root.welt.all. (
3.              2001040901  ; serial
4.              1D          ; refresh
5.              2H          ; retry
6.              1W          ; expiry
7.              2D )        ; minimum
8.
9.              IN NS       gateway
10.             IN MX       10 sonne
11.
12. gateway     IN A        192.168.0.1
13.             IN A        192.168.1.1
14. sonne       IN A        192.168.0.2
15. mond        IN A        192.168.0.3
16. erde        IN A        192.168.1.2
17. mars        IN A        192.168.1.3
```

Datei A.2.5: Datei `/var/named/welt.zone`

Zeile 1: **`$TTL`** definiert die Standard-TTL, die für alle Einträge in dieser Datei gilt, hier 2 Tage (2D = 2 days). TTL bedeutet hier „time to live“, zu deutsch Gültigkeitsdauer.

Zeile 2: Hier beginnt der **`SOA control record`**:

- An erster Stelle steht hier der Name der zu verwaltenden Domain **`welt.all`**, diese ist mit einem '.' abgeschlossen, da ansonsten die Zone noch einmal angehängt würde. Alternativ kann man hier ein **`'@'`** schreiben, dann wird

die Zone dem zugehörigen Eintrag in der `/etc/named.conf` entnommen.

- Nach dem **`IN SOA`** steht der Name des Nameservers, der als Master für diese Zone zuständig ist. In diesem Fall wird der Name **`gateway`** zu **`gateway.welt.all`** ergänzt, da er nicht mit einem `'.'` abgeschlossen ist.
- Danach folgt eine E-Mail-Adresse, der für diesen Nameserver zuständigen Person. Da das `'@'`-Zeichen bereits eine besondere Bedeutung hat, ist hier stattdessen einfach ein `'.'` einzutragen, für **`root@welt.all`** schreibt man hier folglich **`root.welt.all.`**. Den `'.'` am Ende darf man hier nicht vergessen, da sonst die Zone noch angehängt würde.
- Am Ende folgt eine `'('`, um die folgenden Zeilen, bis zur `')'` mit in den SOA-Record einzuschließen.

Zeile 3: Die **`serial number`** ist eine willkürliche Zahl, die bei jeder Änderung an dieser Datei erhöht werden sollte. Sie wird benötigt, um sekundäre Nameserver (Slave-Server) über Änderungen zu informieren. Eingebürgert hat sich dafür eine zehnstellige Zahl aus Datum und fortlaufender Nummer in der Form JJJJMMTTNN.

Zeile 4: Die **`refresh rate`** gibt das Zeitintervall an, in dem Sekundär-Nameserver die **`serial number`** der Zone überprüfen. In diesem Fall 1 Tag (1D = 1 day).

Zeile 5: Die **`retry rate`** gibt den Zeitabstand an, in dem ein sekundärer Nameserver, im Fehlerfall versucht den primären Server erneut zu kontaktieren. Hier 2 Stunden (2H = 2 hours).

Zeile 6: Die **`expiration time`** gibt den Zeitraum an, nachdem ein sekundärer Nameserver die gecacheten Daten verwirft, wenn er keinen Kontakt zum primären Server mehr bekommen hat. Hier ist das eine Woche (1W = 1 week).

Zeile 7: Die **`minimum time to live`** sagt aus, wie lange die Ergebnisse von DNS-Anfragen von anderen Servern gecached werden dürfen, bevor sie ihre Gültigkeit verlieren und neu angefragt werden müssen.

Zeile 9: Das **`IN NS`** gibt den Nameserver an, der für diese Domain zuständig ist. Auch hier gilt, dass **`gateway`** wieder zu **`gateway.welt.all`** ergänzt wird, weil es nicht mit einem `'.'` abgeschlossen ist. Es kann mehrere Zeilen dieser Art geben, eine für den primären und jeweils eine für jeden sekundären Nameserver. Ist für diese Zone **`notify`** in der `/etc/named.conf` nicht auf **`no`** gesetzt, werden alle hier aufgeführten Nameserver über Änderungen der Zonendaten informiert.

Zeile 10: Der MX-Record gibt den Mailserver an, der für die Domain **`welt.all`** die Mails annimmt und weiterverarbeitet oder weiterleitet. In diesem Beispiel ist das der Rechner **`sonne.welt.all`**. Die Zahl vor dem Rechnernamen ist der Präferenz-Wert, gibt es mehrere MX-Einträge, wird zuerst der Mailserver mit dem kleinsten Wert genommen und falls die Auslieferung an diesen scheitert, wird der mit dem nächst höheren Wert versucht.

Zeile 12-17: Das sind jetzt die eigentlichen Adress-Records, in denen den Rechnernamen eine oder mehrere IP-Adressen zugeordnet werden. Die Namen stehen hier ohne abschließenden **.**, da sie ohne angehängte Domain eingetragen sind und alle um **welt.all** ergänzt werden dürfen. Dem Rechner **gateway** sind zwei IP-Adressen zugeordnet, da er über zwei Netzwerkkarten verfügt.

Für die Rückwärts-Auflösung (reverse lookup) von IP-Adressen in Rechnernamen wird die Pseudo-Domain **in-addr.arpa** zu Hilfe genommen. Diese wird dazu an den in umgedrehter Reihenfolge geschriebenen Netzanteil angehängt. Aus **192.168.1** wird dann **1.168.192.in-addr.arpa**; vgl. A.2.6.

```
1. $TTL 2D
2. 1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
3.                          2001040901      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           gateway.welt.all.
10.
11. 1                       IN PTR          gateway.welt.all.
12. 2                       IN PTR          erde.welt.all.
13. 3                       IN PTR          mars.welt.all.
```

Datei A.2.6: Umgekehrte Adress-Auflösung

Zeile 1: $TTL definiert die Standard-TTL, die hier für alle Einträge gilt.

Zeile 2: Der ’revers lookup’ soll mit dieser Datei für das Netz 192.168.1.0 ermöglicht werden. Da die Zone hier ’1.168.192.in-addr.arpa’ heißt, will man dies natürlich nicht an die Rechnernamen anhängen, deshalb sind diese alle komplett mit Domain und abschließendem ’.’ eingetragen. Der Rest entspricht dem, was im vorangegangenen Beispiel für "welt.all", bereits beschrieben wurde.

Zeile 3-7: Siehe vorangegangenes Beispiel für "welt.all".

Zeile 9: Diese Zeile gibt auch hier wieder den Nameserver an, der für diese Zone zuständig ist, diesmal wird aber der Name komplett mit Domain und abschließendem ’.’ hier eingetragen.

Zeile 11-13: Das sind die Pointer-Records, die zu einer IP-Adresse auf den zugehörigen Rechnernamen zeigen. Hier steht am Anfang der Zeile nur die letzte Stelle der IP-Adresse, ohne abschließenden ’.’. Wird jetzt die Zone daran angehängt und man denkt sich das ’.in-addr.arpa’ weg, hat man die komplette IP-Adresse in verdrehter Reihenfolge.

Die Zonendateien sind in dieser Form für Bind8 und Bind9 gleichermaßen verwendbar. Auch Zonentransfers zwischen den verschiedenen Versionen sollten normalerweise kein Problem darstellen.

A.3 DNS Beispielkonfiguration

In der hier vorgeführten Beispiel-Konfiguration eines Nameservers, gehen wir von folgendem Fall aus: Ihre Domain heißt welt.all, Sie haben einen Gateway-Rechner, der die Verbindung zum Internet herstellt und zwei firmeninterne Netze mit einander verbindet. Dieser Rechner wird unser Nameserver und erhält den Namen „gateway“. Ihr Netzwerk sieht wie folgt aus:

Netz 1 enthält die Rechner:

- gateway IP 192.168.1.1
- erde IP 192.168.1.2
- mars IP 192.168.1.3

Netz 2 enthält die Rechner:

- gateway IP 192.168.0.1
- sonne IP 192.168.0.2
- mond IP 192.168.0.3

Die Rechner erde und mars sind nur über gateway mit sonne und mond verbunden, ebenso können alle Rechner nur über gateway das Internet erreichen.

Für die Konfiguration des Nameservers sind folgende Dateien nötig:

named.conf die zentrale Konfigurationsdatei,

welt.zone enthält die host-Tabelle,

192.168.1.zone für das Subnetz mit den Rechnern erde und mars,

192.168.0.zone für das Subnetz mit den Rechnern sonne und mond,

localhost.zone enthält die IP-Adresse des localhost,

127.0.0.zone loopback,

root.hint enthält die Root-Server des Internets.

Die Dateien `localhost.zone`, `127.0.0.zone` und `root.hint` werden automatisch bei der Installation on BIND 8 angelegt.

Die Datei `/etc/named.conf` muss angepasst werden wie in Datei A.3.1 auf der nächsten Seite.

`acl` ist die Zugriffskontroll-Liste, die festlegt, von welchen IP-Adressen aus auf den DNS-Server zugegriffen werden darf.

Der **`directory`**-Eintrag gibt an, wo sich die anderen Konfigurationsdateien befinden. Standard ist `/var/named/`.

`listen-on Port` definiert den Port, von dem der Name Server Anfragen erhält.

```
acl internal { 127.0.0.1; 192.168.1/24; 192.168.0/24; };

options {
     directory "/var/named";
     allow-query { internal; };
#    forwarders { 10.0.0.1; };
#    listen-on port 53 { 127.0.0.1; 192.168.0.1; 192.168.1.1; };
#    query-source address * port 53;
     cleaning-interval 120;
     statistics-interval 0;
     notify no;
};
   zone "welt.all" in {
     type master;
     file "welt.zone";
   };

   zone "0.168.192.in-addr.arpa" in {
     type master;
     file "192.168.0.zone";
   };

   zone "1.168.192.in-addr.arpa" in {
     type master;
     file "192.168.1.zone";
   };

   zone "localhost" in {
     type master;
     file "localhost.zone";
};

   zone "0.0.127.in-addr.arpa" in {
     type master;
     file "127.0.0.zone";
};

   zone "." in {
     type hint;
     file "root.hint";
};
```

Datei A.3.1: Datei `named.conf`

```
$TTL 2D

welt.all. IN SOA       gateway    root.welt.all. (
                       2001040501     ; serial
                       1D             ; refresh
                       2H             ; retry
                       1W             ; expiry
                       2D )           ; minimum

          IN NS        gateway
          IN MX        10 sonne

gateway   IN A         192.168.0.1
          IN A         192.168.1.1
sonne     IN A         192.168.0.2
mond      IN A         192.168.0.3
erde      IN A         192.168.1.2
mars      IN A         192.168.1.3
```

Datei A.3.2: Datei `/var/named/welt.zone`

Die **`zone`**-Einträge geben an, in welchen Konfigurationsdateien die IP-Adressen und Rechnernamen einander zugeordnet werden. Diese Dateien müssen im nächsten Schritt im Verzeichnis `/var/named/` angelegt werden.

In der Datei `welt.zone` (siehe Datei A.3.2) wird die komplette host-Tabelle eingetragen. In unserem Beispiel sieht das wie folgt aus:

Die Option '`$TTL`' gibt die „Time to Live“ also die Gültigkeitsdauer an. '`SOA`' steht für „Start of Authority“ und leitet den vordefinierten Datensatz ein: Rechnername, E-Mail-Adresse, wobei das „@“-Zeichen durch einen „.“ ersetzt wird, Seriennummer (Datum und zweistellige Versionsnummer) und Gültigkeitszeiten. '`NS`' markiert den Name Server. '`A`' signalisiert, dass nun die IP-Adressen der Rechner in der Domain folgen. Der Name-Server „gateway“ hat zwei IP-Adressen, da er zwei Subnetzen angehört. In den beiden weiteren zone-Dateien erfolgt die umgekehrte Adress-Auflösung für die beiden Subnetze; vgl. Beispiel-Dateien A.3.3 auf der nächsten Seite und A.3.4 auf der nächsten Seite.

Bevor Sie nun Ihren Name-Server testen können, muss in der Datei `/etc/rc.config` der Eintrag **`START_NAMED=yes`** gesetzt werden. Anschließend kann man den anderen Rechnern die IP-Adresse des Name-Servers mitteilen, zum Beispiel über YaST1 (Administration des Systems -> Netzwerk konfigurieren -> Konfiguration Nameserver). Wenn Sie nun in einer Konsole **`nslookup erde`** eingeben, sollte Ihnen der Nameserver mit IP-Adresse sowie die IP-Adresse des Rechners erde ausgegeben werden. Sollte der Nameserver nicht funktionieren, finden Sie die Ursache in der Datei `/var/log/messages`.

```
$TTL 2D
0.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
                                2001040501     ; serial
                                1D             ; refresh
                                2H             ; retry
                                1W             ; expiry
                                2D )           ; minimum

          IN NS                 gateway.welt.all.

1         IN PTR                gateway.welt.all.
2         IN PTR                sonne.welt.all.
3         IN PTR                mond.welt.all.
```

Datei A.3.3: Die Datei 192.168.0.zone

```
$TTL 2D
1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
                                2001040501     ; serial
                                1D             ; refresh
                                2H             ; retry
                                1W             ; expiry
                                2D )           ; minimum

          IN NS                 gateway.welt.all.

1         IN PTR                gateway.welt.all.
2         IN PTR                erde.welt.all.
3         IN PTR                mars.welt.all.
```

Datei A.3.4: Die Datei 192.168.1.zone

A.4 Weitere Informationen

- Dokumentation zum Paket `bind8`: `file:/usr/share/doc/packages/bind8/html/index.html`.
- Eine Beispielkonfiguration findet man unter: `/usr/share/doc/packages/bind8/sample-config`
- Manual-Page von **`named`** (**`man 8 named`**), in der die einschlägigen RFCs genannt werden, sowie besonders die Manual-Page von **`named.conf`** (**`man 5 named.conf`**).

B Proxy-Server: Squid

Im folgenden Kapitel wird erläutert, wie das Caching von Webseiten mit Hilfe eines Proxy-Servers funktioniert und welchen Nutzen Squid für Ihr System bietet.

Squid ist der am weitesten verbreitete Proxy-Cache für Linux/UNIX-Plattformen. Wir werden beschreiben, wie er zu konfigurieren ist, welche Systemanforderungen bestehen, wie das eigene System konfiguriert sein muss, um transparentes Proxying durchzuführen, wie man Statistiken über den Nutzen des Cache mithilfe von Programmen wie Calamaris und cachemgr erhält oder wie man Web-Inhalte mit squidgrd filtert.

B.1 Was ist ein Proxy-Cache?

Squid fungiert als Proxy-Cache. Es verhält sich wie ein Makler, der Anfragen von Clients erhält (in diesem Fall Web-Browser) und an den zuständigen Server-Provider weiterleitet. Wenn die angeforderten Objekte beim Vermittler ankommen, behält er eine Kopie davon in einem Festplatten-Cache.

Der Vorteil zeigt sich, wenn mehrere Clients dasselbe Objekt anfordern: Sie können nun direkt aus dem Festplatten-Cache bedient werden, also wesentlich schneller als aus dem Internet. Dies spart gleichzeitig eine Menge Systembandbreite.

Tipp

Squid bietet ein großes Spektrum an Features, z. B. die Festlegung von Hierarchien für die Proxy-Server zum Verteilen der Systemlast, Aufstellen fester Zugriffsregeln an alle Clients, die auf den Proxy zugreifen wollen, Erteilen oder Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen oder die Ausgabe von Statistiken der meistbesuchten Webseiten, wie z. B. das Surfverhalten der Benutzer u. v. m.

Squid ist kein generischer Proxy. Normalerweise vermittelt er nur zwischen HTTP-Verbindungen. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, jedoch keine anderen Internet-Protokolle wie Real Audio, News oder Videokonferenzen. Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Aus diesem Grund werden auch andere Multimedia-Programme nicht unterstützt.

B.2 Informationen zu Proxy-Cache

B.2.1 Squid und Sicherheit

Man kann Squid zusammen mit einer Firewall verwenden, um interne Netzwerke durch den Einsatz von Proxy-Cache nach außen zu schützen. Die Firewall verweigert mit Ausnahme von Squid alle externen Dienste, alle WWW-Verbindungen müssen durch den Proxy aufgebaut werden.

Im Falle einer Firewall-Konfiguration mit einem DMZ würden wir dort unseren Proxy setzen. In diesem Fall ist es wichtig, dass alle Rechner im DMZ ihre Protokolldateien an Rechner innerhalb des gesicherten Netzwerks senden.

Ein Möglichkeit der Implementierung dieser Features mit Hilfe eines so genannten „transparenten“ Proxy wird in Abschnitt B.6 auf Seite 147 behandelt.

B.2.2 Mehrere Caches

Man kann mehrere Caches so konfigurieren, dass Objekte zwischen ihnen ausgetauscht werden können, um die Systemlast zu reduzieren und die Möglichkeit zu steigern, ein bereits im lokalen Netzwerk vorhandenes Objekt zu finden. Möglich sind auch Cache-Hierarchien, so dass ein Cache in der Lage ist, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle herunterzuladen.

Die Wahl der richtigen Topologie für die Cache-Hierarchie ist sehr wichtig, da Netzwerkverkehr insgesamt nicht erhöht werden soll. In einem großen Netzwerk z. B. ist es möglich, für jedes Subnetz einen Proxy-Server zu konfigurieren und diesen dann mit einem übergeordneten Proxy zu verbinden, der wiederum an den Proxy-Cache vom ISP angeschlossen wird.

Die gesamte Kommunikation wird vom ICP (engl. *Internet Cache Protocol*) gesteuert, das auf dem UDP-Protokoll aufgesetzt ist. Der Datenaustausch zwischen Caches geschieht mittels HTTP (engl. *Hyper Text Transmission Protocol*) basierend auf TCP. Allerdings sollten für solche Verbindungen schnellere und einfachere Protokolle verwendet werden, die innerhalb von maximal einer oder zwei Sekunden auf eingehende Anfragen reagieren können.

Um den besten Server für die gewünschten Objekte zu finden, schickt ein Cache an alle Proxies der gleichen Hierarchie eine ICP-Anfrage. Die Proxies werden mittels ICP-Antworten mit dem Code „HIT“ auf die Anfragen reagieren, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Falle mehrerer HIT-Antworten wird der Proxy-Server einen Server für das Herunterladen bestimmen. Diese Entscheidung wird unter anderem dadurch bestimmt, welcher Cache die schnellste Antwort sendet oder welcher näher ist. Bei einer nicht zufrieden stellenden Antwort gesendet wurde, wird die Anfrage an den übergeordneten Cache geschickt.

Tipp

Zur Vermeidung von mehrfacher Speicherung von Objekten in verschiedenen Caches unseres Netzwerks werden andere ICP-Protokolle verwendet, wie z. B. CARP (engl. *Cache Array Routing Protocol*) oder HTCP (engl. *Hyper-Text Cache Protocol*).
Je mehr Objekte sich im Netzwerk befinden, desto leichter wird es, das Gesuchte zu finden.

B.2.3 Zwischenspeichern von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es existieren viele dynamisch generierte CGI-Seiten, Zugriffszähler oder verschlüsselte SSL-Dokumente für eine höhere Sicherheit. Aus diesem Grund werden solche Objekte nicht im Cache gehalten: Bei jedem neuen Zugriff hat sich das Objekt bereits wieder verändert.

Für alle anderen im Cache befindlichen Objekte stellt sich jedoch die Frage, wie lange sie dort bleiben sollen. Für diese Entscheidung werden alle Objekte im Cache drei verschiedenen Stadien zugeordnet:

1. **FRESH:** Wenn dieses Objekt angefordert wird, wird es gesendet, ohne dass ein Abgleich mit dem Originalobjekt im Web stattfindet.
2. **NORMAL:** Der Server, von dem das Objekt ursprünglich stammt, wird daraufhin überprüft, ob sich das Objekt geändert hat. Falls dies der Fall ist, wird die Kopie im Cache aktualisiert.
3. **STALE:** Das Objekt wird als veraltet angesehen und wird neu vom Server heruntergeladen.

Durch Header wie „Last modified“ („zuletzt geändert“) oder „Expires“ („läuft ab“) und dem entsprechenden Datum informieren sich Web- und Proxy-Server über den Status eines Objekts. Es werden auch andere Header verwendet, die z. B. anzeigen, dass ein Objekt nicht zwischengespeichert werden muss.

Objekte im Cache werden normalerweise aufgrund fehlenden Speichers ersetzt, und zwar durch Algorithmen wie LRU (engl. *Last Recently Used*), die zum Ersetzen von Cache-Objekten entwickelt wurden. Das Prinzip besteht im Wesentlichen darin, zuerst die am seltensten gewünschten Objekte zu ersetzen.

B.3 Systemanforderungen

Zuerst sollte die maximale Systemlast bestimmt werden. Es ist wichtig, den Systemspitzen besondere Aufmerksamkeit zu schenken, da diese mehr als viermal so hoch wie der Tagesdurchschnitt sein können. Im Zweifelsfall ist es besser, die

Systemanforderungen zu überschätzen, vorausgesetzt, dass ein am Limit arbeitender Squid zu einem ernsthaften Qualitätsverlust des Dienstes führen kann.

Geordnet nach Wichtigkeit werden in den folgenden Abschnitten die verschiedenen Systemfaktoren aufgezeigt.

B.3.1 Festplatte

Für das Zwischenspeichern spielt Geschwindigkeit eine hohe Rolle. Man sollte sich also um diesen Faktor besonders kümmern. Bei Festplatten ist dieser Parameter als „zufällige Positionierzeit“ in Millisekunden beschrieben. Als Faustregel gilt: Je niedriger dieser Wert, desto besser. Für eine hohe Geschwindigkeit empfiehlt es sich, schnelle Festplatten zu wählen.

Nach dem Squid-Benutzer-Guide (`http://www.squid-cache.org`) ist bei Systemen mit nur einer Festplatte die Formel für die Berechnung der Anzahl von Anfragen pro Sekunde von der Positionierzeit der Festplatten ganz einfach:

Anfragen pro Sekunde = 1000 / Positionierzeit

Squid erlaubt die gleichzeitige Verwendung von mehreren Festplatten und damit eine höhere Anzahl von Anfragen pro Sekunde. Hat man z. B. drei Festplatten mit der gleichen Positionierzeit von 12 Millisekunden, ergibt sich unter Verwendung der vorherigen Formel folgendes:

Anfragen pro Sekunde = 1000 / (Positionierzeit / Anzahl der Festplatten) =
1000 / (12/3) = 250 Anfragen pro Sekunde

Im Vergleich zum Einsatz von IDE-Festplatten sind SCSI-Festplatten zu bevorzugen. Allerdings haben neuere IDE-Festplatten ähnliche Positionierzeiten wie SCSI und zusammen mit DMA-kompatiblen IDE-Controllern erreichen sie eine ähnliche Geschwindigkeit für den Datentransfer ohne dabei die Systemlast beträchtlich zu steigern.

Größe des Festplatten-Cache

In einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (das gewünschte Objekt befindet sich bereits dort) sehr gering, da der Cache schnell gefüllt sein wird. In diesem Fall werden die selten gewünschten Objekte durch neue ersetzt. Steht jedoch `1 GB` für den Cache zur Verfügung und die Benutzer benötigen nur `10 MB` pro Tag zum Surfen, dann dauert es mehr als hundert Tage, bis der Cache voll ist.

Am leichtesten lässt sich die Größe des Cache durch die maximale Übertragungsrate der Verbindung bestimmen. Mit einer Verbindung von `1 MB/Sek` wird die maximale Übertragungsrate bei `125 KB/Sek` liegen. Landet der gesamte Datenverkehr im Cache, kommen innerhalb einer Stunde `450 MB` zusammen. Wenn man nun annimmt, dass der gesamte Datenverkehr lediglich während acht Arbeitsstunden erzeugt wird, erreicht man innerhalb eines Tages `3,6 GB`. Da die Verbindung nicht bis zur Kapazitätsgrenze ausgeschöpft wurde, konnten wir davon ausgehen, dass die gesamte Datenmenge, die durch den Cache geht,

bei ungefähr 2 GB liegt. In unserem Beispiel werden 2 GB Speicher für Squid benötigt, um die Daten aller aufgerufenen Seiten *eines* Tages im Cache zu halten.

Zusammenfassend lässt sich sagen, dass Squid dazu tendiert, kleinere Datenblöcke von der Festplatte zu lesen oder darauf zu schreiben, so dass es wichtiger ist, wie schnell er diese Objekte auf der Festplatte findet, als eine Festplatte mit hohem Durchsatz zu haben.

B.3.2 RAM

Der von Squid benötigte Speicher ist abhängig von der Anzahl der im Cache zugewiesenen Objekte. Squid speichert Cache-Objektverweise und häufig angeforderte Objekte zusätzlich im Speicher, damit diese Daten schneller abgefragt werden können. Der Speicher ist eine Million mal schneller als eine Festplatte!

Jedes Objekt im RAM-Speicher hat eine Größe von 72 Byte (für „kleine“ Pointer-Architekturen wie **Intel**, **Sparc**, **MIPS**; für Alpha sind es 104 Byte), wenn die Durchschnittsgröße eines Objekts im Internet ungefähr 8 KB beträgt und wir 1 GB Festplattenspeicher für den Cache haben, werden wir ungefähr 130.000 Objekte speichern, was alleine für die Meta-Daten fast 10 MB RAM ergibt.

Squid hält auch andere Daten im Speicher, z. B. eine Tabelle mit allen vergebenen IP-Adressen, einen genau festgelegten Domainnamen-Cache, die am häufigsten gewünschten Objekte, Puffer, Zugriffskontrolllisten, etc.

Es ist sehr wichtig, dass ausreichend Speicher für den Squid-Prozess zur Verfügung steht. Sollte er ausgelagert werden müssen, wird sich die Systemleistung nämlich drastisch reduzieren. Für die Cache-Speicherverwaltung wird das Tool cachemgr.cgi verwendet. Es wird im Abschnitt B.7.1 auf Seite 148 erläutert.

B.3.3 CPU

Das Programm Squid benötigt nicht viel CPU. Nur beim Start und während der Überprüfung des Cache-Inhalts ist die Prozessorlast höher. Der Einsatz eines Multiprozessorrechners steigert nicht die Systemleistung. Zur Effektivitätssteigerung ist es besser, schnellere Festplatten zu verwenden oder mehr Speicher hinzuzufügen.

Einige Beispiele von konfigurierten Systemen, auf denen Squid läuft, finden sich unter http://wwwcache.ja.net/servers/squids.html .

B.4 Squid starten

Der Squid auf SuSE Linux ist bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Als Voraussetzung für einen reibungslosen Start sollte das Netzwerk soweit konfiguriert sein, dass mindestens ein Nameserver und sinnvollerweise auch das Internet erreichbar sind. Probleme kann es bereiten, wenn man eine Wählverbindung mit dynamischer DNS-Konfiguration verwendet. In so einem Fall sollte mindestens der Nameserver fest

eingetragen sein, da Squid erst gar nicht startet, wenn er in der `/etc/resolv.conf` keinen DNS findet.

Um Squid zu starten, gibt man auf der Kommandozeile (als `'root'`)

```
rcsquid start
```

ein. Beim ersten Mal wird zunächst die Verzeichnisstruktur in `/var/squid/cache` angelegt. Dies wird vom Startskript `/etc/init.d/squid` automatisch durchgeführt und kann ein paar Sekunden bis Minuten dauern. Erscheint rechts in grün `done`, wurde Squid erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit von Squid sofort testen, indem man im Browser als Proxy `localhost` und `Port 3128` einträgt. Um den Zugriff auf Squid und somit das Internet für alle zu ermöglichen, braucht man in der Konfigurationsdatei `/etc/squid.conf` lediglich den Eintrag `http_access deny all` auf `http_access allow all` zu ändern. Allerdings sollte man dabei bedenken, dass man den Squid damit komplett für jedermann öffnet. Von daher sollte man unbedingt so genannte „ACL's" definieren, die den Zugriff auf den Proxy regeln. Dazu mehr im Abschnitt B.5 auf Seite 145 .

Hat man Änderungen an der Konfigurationsdatei `/etc/squid.conf` vorgenommen, muss man Squid dazu bringen, diese neu einzulesen. Das gelingt mit:

```
rcsquid reload
```

Alternativ kann man Squid auch komplett neu starten:

```
rcsquid restart
```

Wichtig ist noch folgendes Kommando:

```
rcsquid status
```

Damit kann man feststellen, ob der Proxy läuft und mit

```
rcsquid stop
```

wird Squid beendet. Letzteres kann eine Weile dauern, da Squid bis zu einer halben Minute (`shutdown_lifetime`) wartet, bevor die Verbindungen zu den Clients unterbrochen werden und er dann noch seine Daten auf Platte schreiben muss. Beendet man Squid mit einem **`kill`** oder **`killall`**, kann das einen zerstörten Cache zur Folge haben, den man dann löschen muss, um Squid wieder starten zu können.

Beendet sich Squid nach kurzer Zeit, obwohl er scheinbar erfolgreich gestartet wurde, kann das an einem fehlerhaften Nameserver-Eintrag oder einer fehlenden `/etc/resolv.conf` liegen. Den Grund für einen gescheiterten Start protokolliert Squid dabei in der Datei `/var/squid/logs/cache.log` . Soll Squid bereits beim Booten automatisch gestartet werden, braucht man in `/etc/rc.config` lediglich den Eintrag `START_SQUID=no` auf `START_SQUID=yes` abzuändern.

Bei einer Deinstallation von Squid werden weder Cache noch Log-Dateien entfernt. Man muss das Verzeichnis `/var/squid` manuell löschen.

B.5 Die Konfigurationsdatei /etc/squid.conf

Alle Einstellungen zum Squid Proxyserver sind in der Datei `/etc/squid.conf` vorzunehmen. Um Squid erstmalig starten zu können, sind darin keine Änderun-

gen erforderlich, der Zugriff von externen Clients ist jedoch erst einmal gesperrt. Für `localhost` ist der Proxy freigegeben und als Port wird standardmäßig `3128` verwendet. Die Optionen sind ausführlich und mit vielen Beispielen in der vorinstallierten `/etc/squid.conf` dokumentiert. Annähernd alle Einträge sind am Zeilenanfang durch ein #-Zeichen auskommentiert und immer am Ende der zugehörigen Beschreibung zu finden. Die angegebenen Werte entsprechen fast immer den voreingestellten Werten, so dass das Entfernen des Kommentarzeichens, ohne den Parameter der Option zu ändern, bis auf wenige Ausnahmen keine Wirkung hat. Besser ist es, das Beispiel stehen zu lassen und die Option mit dem geänderten Parameter in der Zeile darunter neu einzufügen. So kann man die voreingestellten Werte und Änderungen problemlos nachvollziehen.

Hat man ein Update von einer älteren Squid-Version durchgeführt, ist es unbedingt zu empfehlen, die neue `/etc/squid.conf` zu verwenden und nur die Änderungen von der ursprünglichen Datei zu übernehmen. Versucht man die alte `squid.conf` weiter zu verwenden, läuft man Gefahr, dass die Konfiguration nicht mehr funktioniert, da Optionen immer wieder geändert werden und neue hinzukommen.

Allgemeine Konfigurations-Optionen

http_port 3128 Das ist der Port, auf dem Squid auf Anfragen der Clients lauscht. Voreingestellt ist `3128`, gebräuchlich ist auch `8080`. Es ist möglich, hier mehrere Portnummern, durch Leerzeichen getrennt, anzugeben.

cache_peer <hostname> <type> <proxy-port> <icp-port> Hier kann ein übergeordneter Proxy als „Parent“ eingetragen werden, z. B. wenn man den des Providers nutzen will oder muss. Als `<hostname>` trägt man den Namen bzw. die IP-Adresse des zu verwendenden Proxies und als `<type>` `parent` ein. Für `<proxy-port>` trägt man die Portnummer ein, die der Betreiber des Parent auch zur Verwendung im Browser angibt, meist `8080`. Den `<icp-port>` kann man auf `7` oder `0` setzen, wenn man den ICP-Port des Parent nicht kennt und die Benutzung dieses mit dem Provider nicht vereinbart wurde. Zusätzlich sollte man dann noch `default` und `no-query` nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxy des Providers wie ein normaler Browser.

cache_mem 8 MB Dieser Eintrag gibt an, wie viel Arbeitsspeicher von Squid für das Cachen maximal verwendet wird. Voreingestellt sind `8 MB`.

cache_dir ufs /var/squid/cache 100 16 256 Der Eintrag `cache_dir` gibt das Verzeichnis an, in dem alle Objekte auf Platte abgelegt werden. Die Zahlen dahinter geben den maximal zu verwendenden Plattenplatz in `MB` und die Anzahl der Verzeichnisse in erster und zweiter Ebene an. Den Parameter `ufs` sollte man unverändert lassen. Voreingestellt sind `100 MB` Plattenplatz im Verzeichnis `/var/squid/cache` zu belegen und darin 16 Unterverzeichnisse anzulegen, die jeweils wiederum 256 Verzeichnisse enthalten. Bei Angabe des zu verwendenden Plattenplatzes sollte man genügend Reserven lassen, sinnvoll sind Werte zwischen 50 und maximal 80 Prozent des verfügbaren

Platzes. Die beiden letzten Zahlen für die Anzahl der Verzeichnisse sollte man nur mit Vorsicht vergrößern, da zu viele Verzeichnisse auch wieder auf Kosten der Performance gehen können. Hat man mehrere Platten, auf die der Cache verteilt werden soll, kann man entsprechend viele `cache_dir`-Zeilen eintragen.

cache_access_log /var/squid/logs/access.log Pfadangabe für Log-Datei.

cache_log /var/squid/logs/cache.log Pfadangabe für Log-Datei.

cache_store_log /var/squid/logs/store.log Pfadangabe für Log-Datei.
Diese drei Einträge geben den Pfad zur Protokolldatei von Squid an. Normalerweise wird man daran nichts ändern. Wird der Squid stark beansprucht, kann es sinnvoll sein, den Cache und die Log-Dateien auf verschiedene Platten zu legen.

emulate_httpd_log off Ändert man diesen Eintrag auf `on`, erhält man lesbare Log-Dateien. Allerdings kommen manche Auswerteprogramme damit nicht zurecht.

client_netmask 255.255.255.255 Mit diesem Eintrag kann man die protokollierten IP-Adressen in den Log-Dateien maskieren, um die Identität der Clients zu verbergen. Trägt man hier `255.255.255.0` ein, wird die letzte Stelle der IP-Adresse auf Null gesetzt.

ftp_user Squid@ Hiermit kann man das Passwort setzen, welches Squid für den anonymen FTP-Login verwenden soll. Beim Zugriff auf öffentliche FTP-Server wird im allgemeinen als Login `'anonymous'` und als Passwort die eigene Mail-Adresse verwendet, was das Eingeben von Benutzername und Passwort für jeden FTP-Download erspart. Voreingestellt ist `Squid@` ohne Domain, da die Clients aus beliebigen Domains kommen können. Es kann aber sinnvoll sein, hier eine gültige E-Mail-Adresse in der eigenen Domain anzugeben, da einige FTP-Server diese auf Gültigkeit überprüfen.

cache_mgr webmaster Eine E-Mail-Adresse, an die Squid eine Nachricht schickt, wenn er unerwartet abstürzt. Voreingestellt ist `webmaster`.

logfile_rotate 0 Squid ist in der Lage, die gesicherten Log-Dateien zu rotieren, wenn man **`squid -k rotate`** aufruft. Die Dateien werden dabei, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Dieser Wert steht standardmäßig auf `0`, weil das Archivieren und Löschen der Log-Dateien bei SuSE Linux von einem eigenen Cronjob durchgeführt wird, dessen Konfiguration man in der Datei `/etc/logfiles` findet. Der Zeitraum, nach dem die Dateien gelöscht werden, wird in der `/etc/rc.config` mit dem Eintrag `MAX_DAYS_FOR_LOG_FILES` festgelegt.

append_domain <domain> Mit `append_domain` kann man angeben, welche Domain automatisch angehängt wird, wenn keine angegeben wurde. Meist wird man hier die eigene Domain eintragen, dann genügt es, im Browser `www` einzugeben, um auf den eigenen Webserver zu gelangen.

forwarded_for on Setzt man diesen Eintrag auf `off`, entfernt Squid die IP-Adresse bzw. den Systemnamen des Clients aus den HTTP-Anfragen.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes Normalerweise braucht man diese Werte nicht zu verändern. Hat man aber eine Wählleitung, kann es vorkommen, dass das Internet zeitweilig nicht erreichbar ist. Squid merkt sich dann die erfolglosen Anfragen und weigert sich, diese neu anzufragen, obwohl die Verbindung in das Internet wieder steht. Für diesen Fall sollte man die `minutes` in `seconds` ändern, dann führt auch ein `Reload` im Browser, wenige Sekunden nach der Einwahl, wieder zum Erfolg.

never_direct allow <acl_name> Will man verhindern, dass Squid Anfragen direkt aus dem Internet fordert, kann man hiermit die Verwendung eines anderen Proxies erzwingen. Diesen muss man zuvor unter `cache_peer` eingetragen haben. Gibt man als `<acl_name>` `all` an, erzwingt man, dass sämtliche Anfragen direkt an den `parent` weitergegeben werden. Das kann zum Beispiel nötig sein, wenn man einen Provider verwendet, der die Verwendung seines Proxies zwingend vorschreibt oder die Firewall keinen direkten Zugriff auf das Internet durchlässt.

Optionen zur Zugriffskontrolle

Squid bietet ein ausgeklügeltes System, um den Zugriff auf den Proxy zu steuern. Durch die Verwendung so genannter „ACLs“ ist es einfach und vielseitig konfigurierbar. Dabei handelt es sich um Listen mit Regeln, die der Reihe nach abgearbeitet werden. ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs wie `all` und `localhost` sind bereits vorhanden. Das Festlegen einer ACL an sich bewirkt aber noch gar nichts. Erst wenn sie tatsächlich eingesetzt wird, z. B. in Verbindung mit `http_access`, werden die definierten Regeln abgearbeitet.

acl <acl_name> <type> <data> Eine ACL benötigt zur Definition mindestens drei Angaben. Der Name `<acl_name>` kann frei gewählt werden. Für `<type>` kann man aus einer Vielzahl unterschiedlicher Möglichkeiten auswählen, die man im Abschnitt `ACCESS CONTROLS` in der `/etc/squid.conf` nachlesen kann. Was für `<data>` anzugeben ist, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, z. B. mit Rechnernamen, IP-Adressen oder URLs eingelesen werden. Im folgenden einige einfache Beispiele:

```
acl meinesurfer srcdomain .meine-domain.com
acl lehrer src 192.168.1.0/255.255.255.0
acl studenten src 192.168.7.0-192.168.9.0/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

http_access allow <acl_name> Mit `http_access` wird festgelegt, wer den Proxy verwenden darf und auf was er im Internet zugreifen darf. Dabei sind ACLs anzugeben, `localhost` und `all` sind weiter oben bereits definiert, die mit `deny` oder `allow` den Zugriff sperren oder freigeben. Man kann hier eine Liste mit vielen `http_access`-Einträgen erstellen, die von oben nach unten abgearbeitet werden; je nachdem, was zuerst zutrifft, wird der Zugriff auf die

angeforderte URL freigegeben oder gesperrt. Als letzter Eintrag sollte immer `http_access deny all` stehen. Im folgenden Beispiel hat `localhost`, also der lokale Rechner, freien Zugriff auf alles, während er für alle anderen komplett gesperrt ist:

```
http_access allow localhost
http_access deny all
```

Noch ein Beispiel, in dem die zuvor definierten ACLs verwendet werden: Die Gruppe `'lehrer'` hat jederzeit Zugriff auf das Internet, während die Gruppe `'studenten'` nur Montags bis Freitags, und da nur mittags, surfen darf:

```
http_access deny localhost
http_access allow lehrer
http_access allow studenten mittags
http_access deny all
```

Die Liste mit den eigenen `http_access`-Einträgen sollte man der Übersichtlichkeit halber nur an der dafür vorgesehenen Stelle in der `/etc/squid.conf` eintragen. Das bedeutet zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

und dem abschließenden

```
http_access deny all
```

redirect_program /usr/bin/squidGuard Mit dieser Option kann man einen „redirector“, wie z. B. SquidGuard angeben, der in der Lage ist, unerwünschte URLs zu sperren. In Verbindung mit Proxy-Authentifizierung und den passenden ACLs kann man so den Zugriff auf das Internet für verschiedene Benutzergruppen sehr differenziert steuern. SquidGuard ist ein eigenes Paket, das separat zu installieren und konfigurieren ist.

authenticate_program /usr/sbin/pam_auth Sollen sich die Benutzer am Proxy authentifizieren müssen, kann man hier ein entsprechendes Programm wie z. B. pam_auth angeben. Bei der Verwendung von pam_auth öffnet sich für den Anwender beim ersten Zugriff ein Loginfenster, in dem er Benutzername und Passwort eingeben muss. Zusätzlich ist noch eine ACL erforderlich, damit nur Clients mit gültigem Login surfen können:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Das `REQUIRED` nach `proxy_auth` kann man auch durch eine Liste von erlaubten Benutzernamen oder einen Pfad zu solch einer Liste ersetzen.

ident_lookup_access allow <acl_name> Hiermit erreicht man, dass auf alle durch die ACL definierten Clients eine Ident-Anfrage ausgeführt wird, um die Identität des jeweiligen Benutzers zu ermitteln. Setzt man für `<acl_name>` `all` ein, erfolgt dies generell für alle Clients. Auf den Clients muss dazu ein Ident-Daemon laufen, bei Linux kann man dafür das Paket pidentd installieren, für **Windows** gibt es freie Software, die man sich aus dem Internet besorgen kann. Damit nur Clients mit erfolgreichem Ident-Lookup zugelassen werden, ist auch hier wieder eine entsprechende ACL zu definieren:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Auch hier kann man das `REQUIRED` wieder durch eine Liste erlaubter Benutzernamen ersetzen. Die Verwendung von `Ident` kann den Zugriff merklich verlangsamen, da die Ident-Lookups durchaus für jede Anfrage wiederholt werden.

B.6 Transparente Proxy-Konfiguration

Normalerweise schickt der Web-Browser an einen bestimmten Port des Proxy-Servers Anfragen und der Proxy stellt die angeforderten Objekte zur Verfügung, ob sie nun im Cache sind oder nicht. Innerhalb eines echten Netzwerks können verschiedene Situationen auftreten:

- Aus Sicherheitsgründen ist es besser, wenn alle Clients zum Surfen im Internet einen Proxy verwenden.
- Es ist notwendig, dass alle Clients einen Proxy verwenden, egal ob sie sich dessen bewusst sind oder nicht.
- In großen Netzwerken, die bereits einen Proxy verwenden, ist es möglich, veränderte Konfigurationen der einzelnen Rechner zu speichern, falls sich Änderungen am System ergeben.

In jedem dieser Fälle kann ein transparenter Proxy eingesetzt werden. Das Prinzip ist denkbar einfach: Der Proxy nimmt die Anfragen des Web-Browsers entgegen und bearbeitet sie, sodass der Web-Browser die angeforderten Seiten erhält ohne zu wissen, woher sie kommen. Der gesamte Prozess wird transparent ausgeführt, daher der Name für den Vorgang.

B.6.1 Kernel-Konfiguration

Zuerst sollte sicherstellt sein, dass der Kernel des Proxy-Servers einen transparenten Proxy unterstützt. Andernfalls muss man dem Kernel diese Optionen hinzufügen und ihn neu kompilieren. Weitere Informationen dazu entnehmen Sie bitte dem SuSE Linux Referenzhandbuch.

Wählen Sie im entsprechenden Eintrag zu den Netzwerkoptionen ‘`Network Firewalls`’, und dann die Optionen ‘`IP: firewalling`’ und ‘`IP: Transparent proxying`’. Jetzt muss nur noch die neue Konfiguration gespeichert, der neue Kernel kompiliert und installiert, ggf. LILO neu konfiguriert und das System neu gestartet werden.

B.6.2 Konfigurationsoptionen in /etc/squid.conf

Folgende Optionen in der Datei `/etc/squid.conf` müssen aktiviert werden, um einen transparenten Proxy aufzusetzen:

- **httpd_accel_host** virtual
- **httpd_accel_port** Port 80, an dem der tatsächliche HTTP-Server horcht.
- **httpd_accel_with_proxy** on
- **httpd_accel_uses_host_header** on

Die Standardkonfiguration der Datei `/etc/squid.conf` erlaubt nur Zugriff auf den Proxy von **localhost** aus, deshalb müssen Sie gegebenenfalls weitere Zugriffsregeln definieren;vgl. Abschnitt B.5 auf Seite 145.

B.7 Squid und andere Programme

In diesem Abschnitt wird gezeigt, wie andere Applikationen mit Squid interagieren.

cachemgr.cgi ermöglicht dem Systemadministrator, den benötigten Speicher für das Zwischenspeichern von Objekten zu überprüfen. Squidgrd filtert Webseiten, und calamaris ist ein Berichtsgenerator für Squid.

B.7.1 cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den benötigten Speicher des laufenden Squid-Prozesses. Im Gegensatz zum Protokollieren erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken.

Einrichten

Zuerst wird ein lauffähiger Web-Server auf dem System benötigt. Als Benutzer `'root'` gibt man folgendes eingeben, um herauszufinden, ob Apache bereits läuft: **rcapache status**.

Erscheint eine Nachricht wie diese:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

dann läuft Apache auf unserem Rechner. Andernfalls müssen Sie folgendes eingeben: **rcapache start**

So wird Apache mit den SuSE Linux-Standardeinstellungen gestartet. Weitere Details zu Apache finden sich in diesem Handbuch.

Als letzten Schritt muss man die Datei `cachemgr.cgi` in das Verzeichnis `cgi-bin` von Apache kopieren:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
   /usr/local/httpd/cgi-bin
```

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Cache-Manager ACLs in /etc/squid.conf

Folgende Standardeinstellungen sind für den Cache-Manager erforderlich:

Folgende Regeln sollten enthalten sein:

```
http_access allow manager localhost
http_access deny manager
```

Die erste ACL ist am wichtigsten, da der Cache-Manager versucht, mit dem Squid über das cach_object-Protokoll zu kommunizieren. Die folgenden Regeln setzen voraus, dass der Web-Server und Squid auf demselben Rechner laufen. Die Kommunikation zwischen dem Cache-Manager und Squid entsteht beim Web-Server, nicht beim Browser. Befindet sich der Web-Server also auf einem anderen Rechner, müssen Sie extra eine ACL wie in der Beispieldatei B.7.1 hinzufügen.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP des Webservers
```

Datei B.7.1: Zugriffsregeln

Dann werden noch folgende Regeln aus Datei B.7.2 auf der nächsten Seite benötigt.

Es ist auch möglich, ein Passwort für den Manager zu konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie z. B. Schließen des Cache von Remote oder Anzeigen weiterer Informationen über den Cache. Dann müssen Sie den Eintrag **`cachemgr_passwd`** und die Optionenliste, die angezeigt werden soll, mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragkommentare in `/etc/squid.conf`.

Immer wenn sich die Konfigurationsdatei geändert hat, muss Squid mit dem Kommando **`rcsquid reload`** neu gestartet werden.

Statistiken anzeigen

Gehen Sie zur entsprechenden Web-Seite, z. B.:
`http://webserver.example.org/cgi-bin/cachemgr.cgi`

Drücken Sie auf ‘`continue`’ und lassen Sie sich die verschiedenen Statistiken anzeigen. Weitere Informationen über die einzelnen Einträge, die vom Cache-Manager ausgegeben werden, finden sich in den FAQs zu Squid: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Datei B.7.2: Zugriffsregeln

B.7.2 SquidGuard

Dieses Kapitel soll lediglich eine Einführung zur Konfiguration von SquidGuard sowie ein paar Ratschläge zu dessen Einsatz geben. Auf eine umfangreiche Erklärung wird an dieser Stelle verzichtet. Tiefer gehende Informationen finden sich auf den Webseiten zu SquidGuard: `http://www.squidguard.org`

SquidGuard ist ein freier (GPL), flexibler und ultraschneller Filter, ein Umleiter und „Zugriffs-Controller-PlugIn“ für Squid. Er ermöglicht das Festlegen einer Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen für einen Squid-Cache. SquidGuard verwendet die Standardschnittstelle von Squid zum Umleiten.

squidGuard kann u. a. für Folgendes verwendet werden:

- Beschränkung des Internetzugriffs für einige Benutzer auf bestimmte akzeptierte/bekannte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf bestimmte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf URLs, die bestimmte reguläre Ausdrücke oder Wörter enthalten.
- Umleiten gesperrter URLs an eine „intelligente“ CGI-basierte Infoseite
- Umleiten nicht registrierter Benutzer an ein Registrationsformular.
- Umleiten von Bannern an ein leeres GIF.
- Unterschiedliche Zugriffsregeln abhängig von der Uhrzeit, dem Wochentag, dem Datum etc.
- Unterschiedliche Regeln für die einzelnen Benutzergruppen

Weder mit squidGuard noch mit Squid ist folgendes möglich:

- Text innerhalb von Dokumenten filtern, zensieren oder editieren
- In HTML eingebettete Skriptsprachen wie JavaScript oder VBscript filtern, zensieren und editieren

Verwendung von SquidGuard

Installieren Sie das Paket `squidgrd` aus der Serie `n`. Editieren Sie die Konfigurationsdatei `/etc/squidguard.conf`. Es gibt zahlreiche andere Konfigurationsbeispiele unter `http://www.squidguard.org/config/`. Sie können später mit komplizierteren Konfigurationsenstellungen experimentieren.

Der nächste Schritt besteht darin, eine Dummy-Seite „Zugriff verweigert“ oder eine mehr oder weniger intelligente CGI-Seite zu erzeugen, um Squid umzuleiten, falls der Client eine verbotene Webseite anfordert. Der Einsatz von Apache wird auch hier wieder empfohlen.

Nun müssen wir Squid sagen, dass er SquidGuard benutzen soll. Dafür verwenden wir folgende Einträge in der Datei `/etc/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine andere Option namens **`redirect_children`** konfiguriert die Anzahl der verschiedenen auf dem Rechner laufenden „redirect“, also Umleitungsprozesse (in diesem Fall SquidGuard). SquidGuard ist schnell genug, um eine Vielzahl von Anfragen (SquidGuard ist wirklich schnell: 100.000 Anfragen innerhalb von 10 Sekunden auf einem 500MHz Pentium mit 5900 Domains, 7880 URLs,gesamt 13780) zu bearbeiten. Es wird daher nicht empfohlen, mehr als 5 Prozesse festzusetzen, da die Zuweisung dieser Prozesse unnötig viel Speicher braucht.

```
redirect_children 5
```

Als Letztes senden Sie ein HUP-Signal zum Squid, damit die neue Konfiguration eingelesen wird:

```
rcsquid reload
```

Nun können Sie Ihre Einstellungen in einem Browser testen.

B.7.3 Erzeugen von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, das zur Erzeugung von Aktivitätsberichten des Cache im ASCII- oder HTML-Format verwendet wird. Es arbeitet mit Squid-eigenen Zugriffsprotokolldateien. Die Homepage zu Calamaris befindet sich unter: `http://Calamaris.Cord.de/`

Das Programm ist einfach zu verwenden. Melden Sie sich als `'root'` an und geben Sie folgendes ein:

```
cat access.log.files | calamaris [options] > reportfile
```

Beim Verketten mehrerer Protokolldateien ist die Beachtung der chronologischen Reihenfolge wichtig, d.h. ältere Dateien kommen zuerst.

Die verschiedenen Optionen:

`-a` wird normalerweise zur Ausgabe aller verfügbaren Berichte verwendet, mit

`-w` erhält man einen HTML-Bericht und mit

`-l` eine Nachricht oder ein Logo im Header des Berichts.

Weitere Informationen über die verschiedenen Optionen finden Sie in der Manual Page zu calamaris: **`man calamaris`**

Ein übliches Beispiel:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w >

/usr/local/httpd/htdocs/Squid/squidreport.html
```

Der Bericht wird im Verzeichnis des Web-Servers abgelegt. Wieder wird Apache benötigt, um die Berichte anzeigen zu können.

Ein weiteres, leistungsstarkes Tool zum Erzeugen von Cache-Berichten ist SARG (Squid Analysis Report Generator), das Sie in der Serie n finden. Weitere Informationen dazu gibt es auf der entsprechenden Internetseite unter: http://web.onda.com.br/orso/

B.8 Weitere Informationen zu Squid

Besuchen Sie die Homepage von Squid: http://www.squid-cache.org/. Hier finden Sie den Squid User Guide und eine sehr umfangreiche Sammlung von FAQs zu Squid.

Das Mini-Howto zu einem transparenten Proxy im Paket howtoen, unter: /usr/share/doc/howto/en/mini/TransparentProxy.gz

Des Weiteren gibt es Mailinglisten für Squid unter: squid-users@squid-cache.org.

Das Archiv dazu befindet sich unter: http://www.squid-cache.org/mail-archive/squid-users/

C Sicherheit im Netzwerk

C.1 SSH – secure shell, die sichere Alternative

In unserer Zeit der immer stärkeren Vernetzung werden auch Zugriffe auf entfernte Systeme immer häufiger. Ob elektronische Post abgeholt, ein Server gewartet oder einer Webseite eines Redaktionssystems einen Artikel hinzugefügt wird, immer muss eine Authentifikation der Person erfolgen.

In der Regel sollten Nutzer heutzutage verinnerlicht haben, dass ihr Benutzername und ihr Kennwort lediglich für sie allein gedacht sind. Eine entsprechende Vereinbarung zwischen Arbeitgeber, Rechenzentrum oder Serviceanbieter über die Personengebundenheit dieser Daten ist Standard.

Erschreckend ist demgegenüber die weitgehende Praxis, dass Authentifizierung und Datenübertragung weiterhin in Form von Klartextdaten erfolgt. Die ist beispielsweise der Fall, wenn mit **`Post Office Protocol (POP)`** E-Mail abgeholt wird oder man sich mit **`telnet`** auf einem entfernten System anmeldet. Hierbei gehen die in den Nutzungsbedingungen als sensibel eingestuften Nutzerinformationen und Daten, z. B. der Inhalt eines Briefes, oder ein per talk-Kommando geführtes Gespräch, ohne jeden Schutz offen über das Netzwerk. Dies beeinträchtigt einerseits die Privatsphäre des Nutzers und eröffnet andererseits die Möglichkeit zum Missbrauch eines Zugangs. Insbesondere werden solche Zugänge gern benutzt, um von dort aus andere Systeme anzugreifen, oder Administrator- bzw. Rootrechte auf diesem System zu erlangen.

Jedes an der Weiterleitung der Daten beteiligte oder im gleichen lokalen Netz betriebene Gerät wie Firewall, Router, Switch, Mailserver, Arbeitsplatzrechner, etc., kann die Daten zusätzlich einsehen. Grundsätzlich untersagen zwar die geltenden rechtlichen Regelungen ein solches Vorgehen, stellen es sogar unter Strafe, jedoch sind derartige Angriffe oder unberechtigte Einsichtnahmen nur schwer festzustellen und nachzuweisen.

Die SSH-Software liefert hier den gewünschten Schutz. Die komplette Authentifizierung, in der Regel Benutzername und Passwort, und die Kommunikation erfolgen hier verschlüsselt. Zwar ist auch hier weiterhin das Mitschneiden der übertragenen Daten möglich, doch kann der Inhalt mangels fehlendem Schlüssel durch einen Unwissenden nicht wieder entschlüsselt werden. So wird sichere Kommunikation über unsichere Netze wie das Internet möglich. SuSE Linux bietet in der Serie sec das Paket OpenSSH an.

C.1.1 Das OpenSSH-Paket

Sobald Sie das Paket OpenSSH installiert haben, stehen Ihnen die Programme ssh, scp und sftp als Alternative für telnet, rlogin, rsh, rcp und ftp zur Verfügung.

C.1.2 Das ssh-Programm

Mit dem ssh-Programm können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ist somit gleichermaßen ein Ersatz für telnet und rlogin. Aufgrund der Verwandtschaft zu rlogin zeigt der zusätzliche symbolische Name slogin ebenfalls auf ssh. Zum Beispiel kann man sich mittels

```
hannes@erde:~> ssh sonne
```

auf dem Rechner sonne anmelden. Anschließend wird man nach seinem Passwort auf dem System sonne gefragt:

```
hannes@sonne's password:
```

Nach erfolgreicher Authentifizierung kann dort auf der Kommandozeile oder interaktiv, z. B. mit dem SuSE- Administrationsprogramm YaST, gearbeitet werden. Sollten sich der lokale Benutzername und der auf dem entfernten System unterscheiden, kann ein abweichender Name angegeben werden:

```
hannes@erde:~> ssh -l august sonne
```

oder

```
hannes@erde:~> ssh august@sonne
```

Darüber hinaus bietet ssh die von rsh bekannte Möglichkeit, Kommandos auf einem anderen System auszuführen. Im nachfolgenden Beispiel wird das Kommando **`uptime`** auf dem Rechnersonne ausgeführt und ein Verzeichnis mit dem Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Rechners `erde`.

```
hannes@erde:~> ssh sonne 'uptime; mkdir tmp'
hannes@sonne's password:
  1:21am  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Hochkommata sind hier zum Zusammenfassen der beiden Anweisungen in einem Kommando erforderlich. Nur so wird auch der zweite Befehl auf dem Rechner sonne ausgeführt.

C.1.3 scp – sicheres Kopieren

Mittels scp kopieren Sie Dateien auf einen entfernten Rechner. scp ist der sichere, verschlüsselte Ersatz für rcp. Zum Beispiel kopiert

```
hannes@erde:~> scp MeinBrief.tex sonne:
```

die Datei `MeinBrief.tex` vom Rechner `erde` auf den Rechner `sonne`. Insoweit sich die beteiligten Nutzernamen auf `erde` und `sonne` unterscheiden, muss bei scp auf die bereits zum ssh-Kommando beschriebene Schreibweise **`Nutzername@Rechnername`** zurückgegriffen werden. Eine Option **`-l`** existiert nicht.

Nachdem das Passwort eingegeben wurde, beginnt scp mit der Datenübertragung und zeigt dabei den Fortschritt anhand eines von links nach rechts anwachsenden Balkens aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (engl. *estimated time of arrival*) angezeigt. Jegliche Ausgabe kann durch die Option **`-q`** unterdrückt werden.

scp bietet neben dem Kopieren einzelner Dateien ein rekursives Verfahren zum Übertragen ganzer Verzeichnisse.

```
hannes@erde:~> scp -r src/ sonne:backup/
```

kopiert den kompletten Inhalt des Verzeichnisses `src/` inklusive aller Unterverzeichnisse auf den Rechner `sonne` und dort in das Unterverzeichnis `backup/`. Dieses wird automatisch angelegt wenn es fehlt.

Mittels der Option **`-p`** kann scp die Zeitstempel der Dateien erhalten. **`-C`** sorgt für eine komprimierte Übertragung. Dadurch wird einerseits das zu übertragende Datenvolumen minimiert, andererseits aber ein höherer Rechenaufwand erforderlich.

C.1.4 sftp - sicherere Dateiübertragung

Alternativ kann man zur sicheren Datenübertragung sftp verwenden. sftp bietet innerhalb der Sitzung viele der von ftp bekannten Kommandos. Gegenüber scp mag es vor allem beim Übertragen von Daten, deren Dateinamen unbekannt sind, von Vorteil sein.

C.1.5 Der SSH Daemon (sshd) – die Serverseite

Damit ssh und scp, die Clientprogramme des SSH-Paketes, eingesetzt werden können, muss im Hintergrund der SSH-Daemon, ein Server, laufen. Dieser erwartet seine Verbindungen auf **`TCP/IP Port 22`**.

Der SSH-Daemon ist Bestandteil des SSH-Paketes und wird in einem SuSE Linux System automatisch in `Runlevel 3` und `5` gestartet. n `/etc/rc.config` ist die Variable `START_SSHD` dazu auf `yes` voreingestellt.

Während des ersten Starts generiert der Daemon zwei Schlüsselpaare. Die Schlüsselpaare bestehen aus einem privaten und einem öffentlichen (engl. *public*) Teil. Deshalb bezeichnet man dies als ein public-key basiertes Verfahren. Um die Sicherheit der Kommunikation mittels SSH zu gewährleisten, darf ausschließlich der Systemadministrator die Dateien der privaten Schlüssel einsehen können. Die Dateirechte werden per Voreinstellung entsprechend restriktiv gesetzt. Die privaten Schlüssel werden lediglich lokal vom SSH-Daemon benötigt und dürfen an niemanden weitergegeben werden. Demgegenüber werden die öffentlichen Schlüsselbestandteile (an der Namensendung `.pub` erkennbar) an Kommunikationspartner weitergegeben und sind entsprechend für alle Benutzer lesbar.

Eine Verbindung wird vom SSH-Client eingeleitet. Der wartende SSH-Daemon und der anfragende SSH-Client tauschen Identifikationsdaten aus, um die Protokoll- und Softwareversion abzugleichen und die Verbindung zu einem falschen Port auszuschließen. Da ein Kindprozess des ursprünglichen SSH-Daemons antwortet, sind gleichzeitig viele SSH-Verbindungen möglich.

Der Server sendet sodann seinen öffentlichen **`host key`** und einen stündlich vom SSH-Daemon neu generierten **`server key`**. Mittels beider verschlüsselt (engl. *encrypt*) der SSH-Client einen von ihm frei gewählten Sitzungsschlüssel (engl. *session key*) und sendet ihn an den SSH-Server. Er teilt dem Server zudem die gewählte Verschlüsselungsmethode (engl. *cipher*) mit.

Die zur Entschlüsselung des Sitzungsschlüssels zwingend erforderlichen privaten host und server keys, können nicht aus den öffentlichen Teilen abgeleitet

werden. Somit kann allein der kontaktierte SSH-Daemon mit seinen privaten Schlüsseln den Sitzungsschlüssel entziffern (vgl. `/usr/share/doc/packages/openssh/RFC.nroff`). Diese einleitende Phase der Verbindung kann man mittels der Fehlersuchoption **`-v`** des SSH-Clientprogramms gut nachvollziehen. Sie endet mit der Bestätigung „Received encrypted confirmation.“ des SSH-Daemons. Indem der Client alle öffentlichen host keys nach der ersten Kontaktaufnahme in `~/.ssh/known_hosts` ablegt, können so genannte „man-in-the-middle“-Angriffe unterbunden werden. SSH-Server, die versuchen, Name und IP-Adresse eines anderen vorzutäuschen, werden durch einen deutlichen Hinweis enttarnt. Sie fallen entweder durch einen gegenüber `~/.ssh/known_hosts` abweichenden host-Schlüssel auf, oder können mangels passendem privaten Gegenstück den vereinbarten Sitzungschlüssel nicht entschlüsseln.

Es empfiehlt sich, die in `/etc/ssh/` abgelegten privaten und öffentlichen Schlüssel extern und gut geschützt zu archivieren. So können Änderungen der Schlüssel festgestellt und nach einer Neuinstallation die alten wieder eingespielt werden. Dies erspart den Benutzern die beunruhigende Warnung. Ist es sichergestellt, dass es sich trotz der Warnung um den korrekten SSH-Server handelt, muss der vorhandene Eintrag zu diesem System aus `~/.ssh/known_hosts` entfernt werden.

C.1.6 SSH-Authentifizierungsmechanismen

Jetzt erfolgt die eigentliche Authentifizierung, die in ihrer einfachsten Weise aus der Eingabe eines Passwortes besteht, wie es in den oben aufgezeigten Beispielen erfolgte. Ziel von SSH war die Einführung einer sicheren, aber zugleich einfach zu nutzenden Software. Wie bei den abzulösenden Programmen rsh und rlogin muss deshalb auch SSH eine im Alltag einfach zu nutzende Authentifizierungsmethode bieten. SSH realisiert dies mittels eines weiteren hier vom Nutzer erzeugten Schlüsselpaares. Dazu liefert das SSH-Paket das Hilfsprogramm ssh-keygen mit. Nach der Eingabe von

```
hannes@sonne:~> ssh-keygen
Generating RSA keys:
```

wird das Schlüsselpaar generiert und der Basisdateiname zur Ablage der Schlüssel erfragt:

```
Enter file in which to save the key (/home/hannes/.ssh/identity):
```

Bestätigen Sie die Voreinstellung und beantworten Sie die Frage nach einer Passphrase:

```
Enter passphrase (empty for no passphrase):
```

Auch wenn die Software eine leere Passphrase nahelegt, sollte bei der hier vorgeschlagenen Vorgehensweise ein Text von zehn bis 30 Zeichen Länge gewählt werden. Verwenden Sie möglichst keine kurzen und einfachen Worte oder Sätze. Nach erfolgter Eingabe wird zur Bestätigung eine Wiederholung der Eingabe verlangt. Anschließend wird der Ablageort des privaten und öffentlichen Schlüssels, in unserem Beispiel der Dateien `identity` und `identity.pub`, ausgegeben.

```
Enter same passphrase again:
Your identification has been saved in /home/hannes/.ssh/identity.
Your public key has been saved in /home/hannes/.ssh/identity.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 hannes@sonne
```

Insbesondere, wenn der private Schlüssel (identity) auf einem nicht von Ihnen selbst administrierten System erzeugt wird und abgelegt ist, oder Sie Ihr Benutzerverzeichnis per NFS beziehen, sollten Sie eine Passphrase benutzen. Verwenden Sie **`ssh-keygen -p`** , um Ihre alte Passphrase zu ändern.

Kopieren Sie den öffentlichen Teil des Schlüssels (identity.pub) auf den entfernten Rechner und legen Sie ihn dort als `~/.ssh/authorized_keys` ab. Zur Authentifizierung werden Sie beim nächsten Verbindungsaufbau nach Ihrer Passphrase gefragt. Sollte dies nicht der Fall sein, überprüfen Sie bitte Ort und Inhalt der zuvor erwähnten Dateien.

Auf Dauer ist diese Vorgehensweise mühsamer, als die Eingabe eines Passwortes. Entsprechend liefert das SSH-Paket ein weiteres Hilfsprogramm, den ssh-agent, der für die Dauer einer „X-session“ private Schlüssel bereit hält. Dazu wird das gesamte X als Kindprozess des ssh-agents gestartet. Sie erreichen dies am einfachsten, indem Sie am Anfang der Datei `.xsession` die Variable `usessh` auf `yes` setzen und sich über einen Displaymanager, z. B. KDM oder XDM, anmelden. Alternativ können Sie ssh-agent startx verwenden.

Sobald Ihre X-session gestartet ist, schalten Sie Ihren privaten Schlüssel mittels ssh-add frei. Insoweit ssh-add nicht auf ein Terminal zugreifen kann, z. B. über ein Menü aufgerufen wird, oder eine Eingabeumleitung von **`</dev/null`** erfolgt, erscheint eine grafische Eingabeaufforderung `x11-ssh-askpass`. Nun können Sie wie gewohnt ssh oder scp nutzen. Insoweit Sie Ihren privaten Schlüssel wie zuvor verteilt haben, sollten Sie jetzt nicht mehr nach dem Passwort gefragt werden. Achten Sie beim Verlassen Ihres Rechner darauf, dass Sie Ihre X-session beenden oder mittels einer passwortgeschützten Bildschirmsperre, z. B. xlock, verriegeln.

C.1.7 X-, Authentifizierungs- und sonstige Weiterleitung

Über die bisher beschriebenen sicherheitsrelevanten Verbesserungen hinaus erleichtert ssh auch die Verwendung von entfernten X-Anwendungen. Insoweit Sie **`ssh`** mit der Option **`-X`** aufrufen, wird auf dem entfernten System automatisch die DISPLAY-Variable gesetzt und alle X-Ausgaben werden durch die bestehende ssh-Verbindung auf den Ausgangsrechner weitergeleitet. Diese bequeme Funktion unterbindet gleichzeitig die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch die gesetzte Option **`-A`** wird der ssh-agent-Authentifizierungsmechanismus auf den nächsten Rechner mit übernommen. Man kann so von einem Rechner zum anderen gehen, ohne ein Passwort eingeben zu müssen. Allerdings nur, wenn man zuvor seinen öffentlichen Schlüssel auf die beteiligten Zielrechner verteilt und korrekt abgelegt hat.

Beide Mechanismen sind vorsichtshalber in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/sshd_config`

oder der nutzereigenen `~/.ssh/config` permanent eingeschaltet werden.

Analog zur X-Weiterleitung kann man ssh zur beliebigen Umleitung von TCP/IP-Verbindungen benutzen. Als Beispiel sei hier die Weiterleitung des SMTP- und POP3-Ports aufgeführt:

```
root@erde:~ # ssh -L 25:sonne:25 sonne
```

Hier wird jede Verbindung zu „`erde` Port 25“, SMTP auf den SMTP-Port von `sonne` über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere für Nutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Fähigkeiten von Nutzen. Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den „heimischen“ Mailserver übertragen werden.

Analog leitet

```
root@erde:~ # ssh -L 110:sonne:110 sonne
```

alle Port 110, POP3-Anfragen an `erde` auf den POP3-Port von `sonne` weiter.

Beide Beispiele müssen Sie als Nutzer `'root'` ausführen, da auf privilegierte lokale Ports verbunden wird. Bei bestehender SSH-Verbindung wird die Post wie gewohnt als normaler Nutzer versandt und abgeholt. Der SMTP- und POP3-Host muss dabei auf localhost konfiguriert werden.

Zusätzliche Informationen können den Manualpages der einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh` entnehmen werden.

C.2 Sicherheit ist Vertrauenssache

C.2.1 Grundlagen

Eines der grundlegendsten Leistungsmerkmale eines Linux/Unix-Systems ist, dass mehrere Benutzer (multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben Rechner (multi-tasking) ausführen können. Das Betriebssystem ist darüber hinaus netzwerktransparent, sodass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Applikationen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bezogen werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt verwaltet werden können. Hier geht es unter anderem auch um Sicherheit und den Schutz der Privatsphäre. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten weiterhin verfügbar sein, auch wenn solche Defekte womöglich den vorübergehenden Ausfall einer größeren Infrastruktur zur Folge hatten.

Auch wenn sich dieses Kapitel des SuSE-Handbuchs in der Hauptsache mit der Vertraulichkeit der Daten und dem Schutz der Privatsphäre der Benutzer beschäftigt, sei betont, dass ein umfassendes Sicherheitskonzept als integralen Bestandteil immer ein regelmäßiges, funktionierendes und überprüftes Backup beinhaltet. Ohne dieses Backup der Daten wird es nicht nur im Fall eines Hardware-Defekts schwierig sein, weiterhin auf die Daten zuzugreifen, sondern insbeson-

dere auch dann, wenn nur der Verdacht besteht, dass jemand sich unbefugterweise an den Daten zu schaffen gemacht hat.

C.2.2 Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- Persönliche Kommunikation mit jemand, der über die gewünschten Informationen verfügt bzw. Zugang zu bestimmten Daten auf einem Computer hat,
- direkt an der Console eines Rechners (physikalischer Zugriff),
- über eine serielle Schnittstelle oder
- über ein Netzwerk.

Alle diese Fälle sollten eine Gemeinsamkeit haben: Sie sollten sich als Benutzer authentifizieren müssen, bevor Sie Zugriff auf die Ressourcen oder Daten bekommen. Ein Webserver mag da anders geartet sein, aber Sie wollen sicherlich nicht, dass der Webserver Ihre persönlichen Daten an Surfer preisgibt. Eine SuSE-Linux Installation ließe sich mit wenigen Handgriffen dazu bringen, Sie nach dem Systemstart direkt und ohne Passwort mit Ihrer Arbeitsoberfläche zu konfrontieren, aber dieses Vorgehen ist meistens unangemessen. Damit könnte jemand in Ihrem Namen Daten manipulieren und Programme ausführen.

Der erste Fall der oben genannten ist der menschlichste von allen: Etwa bei einer Bank müssen Sie einem Angestellten beweisen, dass Ihnen der Zugriff auf Ihre Konten gestattet ist, indem Sie mit Ihrer Unterschrift, einer PIN oder mit einem Passwort beweisen, dass Sie derjenige sind, für den Sie sich ausgeben. In manchen Fällen kann es gelingen, durch das Erwähnen von Kenntnissen oder durch geschickte Rhetorik das Vertrauen eines Wissensträgers zu erschleichen, so dass dieser weitere Information preisgibt, womöglich ohne dass das Opfer dies bemerkt.

Manche Menschen sind so unvorsichtig mit ihren Äußerungen und unbewusst mit ihren Antworten, dass auch die Antworten, die sie für nicht beantwortet halten, genug Information enthalten, um Fragen immer präziser zu stellen, weil wie in einem Mosaik immer mehr Details bekannt werden. („Nein, der Herr Meier ist im Urlaub und kommt erst in drei Wochen wieder. Und im übrigen ist er nicht mein Chef, zumal er im vierten Stock sitzt und ich im dritten!“) Man nennt dies in Hackerkreisen „Social Engineering“. Gegen diese Art von Angriff hilft nur Aufklärung und ein bewusster Umgang mit Information und Sprache. Einbrüchen auf Rechnersystemem geht oft eine Art Social-Engineering-Angriff, etwa auf das Empfangspersonal, Dienstleister in der Firma oder auch Familienmitglieder, voraus, der erst viel später bemerkt wird.

Jemand, der (unbefugt) Zugriff auf Daten erlangen will, könnte auch die traditionellste Methode benutzen, denn die Hardware selbst ist ein Angriffspunkt. Der Rechner muss gegen Entnahme, Austausch und Sabotage von Teilen und Gesamteinheit (und dem Backup der Daten!) sicher verstaut sein - dazu kann auch eine eventuell vorhandene Netzwerkleitung oder ein Stromkabel gehören. Außerdem muss der Startvorgang muss abgesichert sein, denn allgemein bekannte

Tastenkombinationen können den Rechner zu speziellen Reaktionen veranlassen. Dagegen hilft das Setzen von BIOS- und Bootloaderpasswörtern.

Serielle Schnittstellen mit seriellen Terminals sind heute zwar immer noch gebräuchlich, werden aber kaum noch an neuen Arbeitsplätzen installiert. Ein serielles Terminal stellt eine besondere Art des Zugriffs dar: Es ist keine Netzwerkschnittstelle, da kein Netzwerkprotokoll zur Kommunikation zwischen den Systemeinheiten verwendet wird. Ein simples Kabel (oder eine Infrarotschnittstelle) wird als Übertragungsmedium für einfache Zeichen verwendet. Das Kabel selbst ist dabei der einfachste Angriffspunkt: Man muss nur einen alten Drucker daran anschließen und kann die Kommunikation aufzeichnen. Was mit einem Drucker möglich ist, geht selbstverständlich mit beliebigem Aufwand auch anders.

Netzwerke vereinfachen uns den Zugriff auf Daten mit zum Teil komplexen Kommunikationsprotokollen. Das mag paradox klingen, muss aber so sein. Wenn Sie völlig vom Ort unabhängig sein wollen und einen Rechner fernsteuern oder Daten von ihm beziehen wollen, dann brauchen Sie abstrakte, modulare Modelle, deren Ebenen weitgehend voneinander unabhängig sind. Im täglichen Umgang mit Computern begegnen Sie ständig solchen Modellen: Modularität ist, wenn Ihr Textverarbeitungsprogramm nicht wissen muss, welche Art von Festplatte Sie haben, und Ihr E-Mail-Programm sollte sich nicht darum kümmern müssen, ob Sie nun ein Modem oder eine Ethernet-Karte haben. Teile Ihres Betriebssystems (in unserem Fall Linux) stellen Ihnen die Funktionalität mittels einer definierten Schnittstelle zur Verfügung und kümmern sich um die Details. So kann einerseits ein Textverarbeitungsprogramm oder ein Mail-User-Agent (MUA) auch auf Rechnern mit gänzlich unterschiedlicher Hardware funktionieren, und andererseits können sie von einem beliebigen Ort aus betrieben werden, die nötige technische Ausstattung vorausgesetzt.

In Hinblick auf die Daten bedeutet dies, dass es keinen Unterschied macht, ob eine Datei in der Kommandozeile geöffnet oder mit einem Webbrowser betrachtet wird. Genauso kann man sich über ein Netzwerk (etwa mit einem telnet-Programm oder, viel besser, mit einem secure shell Programm (ssh), das den Netzverkehr vollständig verschlüsselt) einloggen und die Datei lesen. Dennoch müssten dabei mehrere Hürden übersprungen werden. Zunächst müssen Netzwerk und Rechner verbunden werden, dann muss sich der Benutzer authentifizieren (die Identität nachweisen). Dabei schränken schließlich noch die Zugriffsrechte der Datei die Handlungsmöglichkeiten ein.

Da das Öffnen einer Datei auf einem Rechner anderen Zugriffsbeschränkungen unterliegt als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem Rechner, ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie ist da markiert, wo Daten in Pakete verschnürt werden müssen, um verschickt zu werden und zur Anwendung zu gelangen.

Lokale Sicherheit

Lokale Sicherheit mit den physikalischen Gegebenheiten, in denen der Rechner aufgestellt ist. Wir gehen davon aus, dass Sie Ihren Rechner so aufgebaut haben, dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt.

In Bezug auf „Lokale Sicherheit“ besteht die Aufgabe darin, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder oder die Identität eines anderen Benutzen annehmen kann. Dies gilt im Allgemeinen, im Speziellen sind natürlich besonders `'root'`-Rechte gemeint, da der Benutzer `'root'` im System Allmacht hat; er kann unter anderem ohne Passwort zu jedem lokalen Benutzer werden und jede lokale Datei lesen.

Die Liste der Möglichkeiten, ein System anzugreifen, wenn man bereits Zugriff auf lokale Ressourcen über die Kommandozeile hat, ist recht lang.

Passwörter

Ihr Linux-System speichert Passwörter nicht etwa im Klartext ab und vergleicht ein eingegebenes Passwort mit dem, was gespeichert ist. Bei einem Diebstahl der Datei, in der die Passwörter stehen, wären dann ja alle Accounts auf Ihrem System kompromittiert. Stattdessen wird Ihr Passwort verschlüsselt abgelegt und jedes Mal, wenn Sie das Passwort eingegeben haben, wird dieses wieder verschlüsselt und das Ergebnis verglichen mit dem, was als verschlüsseltes Passwort abgespeichert ist. Dies macht natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht das Klartextpasswort errechnen kann. Dies erreicht man durch so genannte „Falltüralgorithmen“, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach zurückrechnen und das Passwort sehen, sondern er muss alle möglichen Buchstabenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie Ihres. Bei acht Buchstaben pro Passwort gibt es beträchtlich viele Kombinationen.

Mit ein Argument für die Sicherheit dieser Methode in den 70er Jahren war, dass der verwendete Algorithmus recht langsam ist und Zeit im Sekundenbereich für das verschlüsseln von einem Passwort brauchte. Heutige PCs schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund dürfen verschlüsselte Passwörter nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar), und die Passwörter dürfen nicht leicht zu erraten sein, für den Fall, dass die verschlüsselten Passwörter wegen eines Fehlers eben doch sichtbar werden. Ein Passwort wie „Phantasie“ umzuschreiben in „Ph@nt@s13“ hilft nicht viel: Solche Vertauschungsregeln können von Knackprogrammen, die Wörterbücher zum Raten benutzen, sehr leicht aufgelöst werden. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für den Benutzer eine persönliche Bedeutung haben, etwa die Anfangsbuchstaben der Wörter eines Satzes, oder nehmen Sie zum Beispiel einen Buchtitel wie „Der Name der Rose“ von Umberto Eco. Daraus gewinnen Sie ein gutes Passwort: „DNdRvUE9“. Ein Passwort wie „Bierjunge“ oder „Jasmin76“ würde schon jemand erraten können, der Sie oberflächlich gut kennt.

Der Bootvorgang

Verhindern Sie, dass mit einer Diskette oder einer CD-ROM gebootet werden kann, indem Sie die Laufwerke ausbauen oder indem Sie ein BIOS-Passwort

setzen und im BIOS ausschließlich das Booten von Festplatte erlauben.

Linux Systeme starten gewöhnlicherweise mit einem Boot-loader, der es erlaubt, zusätzliche Optionen an den zu startenden Kernel weiterzugeben. Solche Optionen sind im hohem Maße sicherheitskritisch, weil der Kernel ja nicht nur mit `'root'`-Rechten läuft, sondern die `'root'`-Rechte von Anfang an vergibt. Verhindern Sie, dass jemand solche Optionen verwendet, während Ihr Rechner startet, indem Sie die Optionen „restricted“ und „password=irgendein_passwort“ in `/etc/lilo.conf` verwenden. Vergessen Sie nicht, das Kommando **`lilo`** auszuführen, wenn Sie die Datei `/etc/lilo.conf` verändert haben, und achten Sie auf die Ausgaben des Programms! Wenn Sie das Passwort vergessen, müssen Sie das BIOS-Passwort kennen und von CD booten, um den Eintrag in `/etc/lilo.conf` aus einem Rettungssystem heraus zu lesen.

Zugriffsrechte

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für eine jeweilige Aufgabe zu arbeiten. Es ist definitiv nicht nötig, seine E-Mails als root zu lesen und zu schreiben. Wenn das Mailprogramm (MUA = Mail User Agent), mit dem Sie arbeiten, einen Fehler hat, dann wirkt sich dieser Fehler mit genau den Rechten aus, die Sie zum Zeitpunkt des des Angriffs hatten. Hier geht es also auch um Schadensminimierung.

Die einzelnen Rechte der weit über 200.000 Dateien einer SuSE-Distribution sind sorgfältig vergeben. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien nur unter größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Rechte der Dateien achten. Erfahrene und sicherheitsbewusste Admins verwenden bei dem Kommando **`ls`** stets die Option **`-l`** für eine ausführliche Liste der Dateien mitsamt den Zugriffsrechten, so dass sie eventuell falsch gesetzte Dateirechte gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können, sondern auch dass die veränderten Dateien von `'root'` ausgeführt oder im Fall von Konfigurationsdateien von Programmen als `'root'` benutzt werden können. Damit könnte ein Angreifer seine Rechte beträchtlich ausweiten. Man nennt solche Angriffe dann Kukukseier, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kukuk seine Eier von fremden Vögeln ausbrüten lässt.

SuSE-Systeme verfügen über die Dateien `permissions`, `permissions.easy`, `permissions.secure` und `permissions.paranoid` im Verzeichnis `/etc`. In diesen Dateien werden besondere Rechte wie etwa welt-schreibbare Verzeichnisse oder für Dateien setuser-ID-bits festgelegt, d.h. das Programm läuft dann nicht mit der Berechtigung des Eigentümers des Prozesses, der es gestartet hat, sondern mit der Berechtigung des Eigentümers der Datei, und das ist in der Regel `'root'`. Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Änderungen festhalten kann. Die Variable **`PERMISSION_SECURITY`** aus der Datei `/etc/rc.config` legt fest, welche der Dateien für Konfigurationsprogrammen von SuSE zur Vergabe der Rechte benutzt werden sollen. Diese Auswahl können Sie auch komfortabel unter dem Menüpunkt `'Sicherheit'` von YaST1 und YaST2 treffen. Mehr zu diesem The-

ma erfahren Sie direkt aus der Datei `/etc/permissions` und der Manpage des Kommandos **`chmod`** (**`man chmod`**).

file race conditions

Ein Programm will eine Datei in einem Verzeichnis anlegen, welches für jedermann schreibbar ist (wie `/tmp`). Es überprüft, ob die Datei bereits existiert und erzeugt die Datei, wenn sie noch nicht vorhanden war. Zwischen dem Überprüfen der Existenz und dem Anlegen der Datei vergeht aber eine kurze Zeit, in der ein Angreifer einen symbolischen Link anlegen kann, einen Zeiger auf eine andere Datei. Das Programm verfolgt dann diesen symbolischen Link und überschreibt dabei die Zieldatei mit seinen Privilegien. Dies ist ein Rennen ((engl. *race*)), weil für den Angreifer nur eine kurze Zeit bleibt, in der er den „symlink“ anlegen kann. Dieses Rennen ist nur dann möglich, wenn der Vorgang von Überprüfen und Anlegen einer Datei nicht atomisch, also unteilbar ist. Wenn das Rennen stattfinden kann, dann kann es von einem Angreifer auch gewonnen werden, das ist eine Frage der Wahrscheinlichkeit.

Buffer overflows, format string bugs

Wann immer ein Programm Daten verarbeitet, die in beliebiger Form unter Einfluss eines Benutzers stehen oder standen, ist besondere Vorsicht geboten. Diese Vorsicht gilt in der Hauptsache für den Programmierer der Anwendung: Er muss sicherstellen, dass die Daten durch das Programm richtig interpretiert werden, dass die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind und dass er die Daten in konsistenter Art und Weise durch sein eigenes Programm und die dafür definierten Schnittstellen weiterreicht.

Ein „Buffer Overflow“ passiert dann, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer eigentlich ist. Es könnte sein, dass die Daten (die vom Benutzer kamen) etwas mehr Platz verlangen, als im Puffer zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenze hinaus ist es unter Umständen möglich, dass ein Programm aufgrund der Daten, die er eigentlich nur verarbeiten soll, Programmsequenzen ausführt, die unter dem Einfluss des Users und nicht des Programmierers stehen. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Rechten abläuft (siehe Abschnitt C.2.2 auf der vorherigen Seite). „Format String Bugs“ funktionieren etwas anders, verwenden aber wieder user-input, um das Programm von seinem eigentlichen Weg abzubringen.

Diese Programmierfehler werden normalerweise bei Programmen ausgebeutet (engl. *exploit*), die mit gehobenen Privilegien ausgeführt werden, also setuid- und setgid-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte von den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe Abschnitt C.2.2 auf der vorherigen Seite).

Da „Buffer Overflows“ und „Format String Bugs“ Fehler bei der Behandlung von Benutzerdaten sind, sind sie nicht notwendigerweise nur ausbeutbar, wenn

man bereits Zugriff auf ein lokales „login“ hat. Viele der bekannt gewordenen Fehler können über eine Netzwerkverbindung ausgenutzt werden. Deswegen sind „Buffer Overflows“ und „Format String Bugs“ nicht direkt auf den lokalen Rechner oder das Netzwerk klassifizierbar.

Viren

Entgegen andersartiger Verlautbarungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als „Proof-of-Concept“ geschrieben worden, als Beweis, dass die Technik funktioniert. Allerdings ist noch keiner dieser Viren in „freier Wildbahn“ beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt, ohne den sie nicht überlebensfähig sind. Dieser Wirt ist ein Programm oder ein wichtiger Speicherbereich für das System, etwa der Master-Boot-Record, und er muss für den Programmcode des Virus beschreibbar sein. Linux hat aufgrund seiner Multi-User Fähigkeiten die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, also insbesondere Systemdateien. Wenn Sie als `'root'` arbeiten, erhöhen Sie also die Wahrscheinlichkeit, dass Ihr System von solch einem Virus infiziert wird. Berücksichtigen Sie aber die Regel der geringstmöglichen Privilegien, ist es Schwierigkeiten unter Linux einen Virus zu bekommen. Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie aus dem Internet bezogen haben und dessen genaue Herkunft Sie nicht kennen. SuSE-rpm Pakete sind kryptographisch signiert und tragen mit dieser digitalen Unterschrift das Markenzeichen der Sorgfalt beim Bau der Pakete bei SuSE. Viren sind klassische Symptome dafür, dass auch ein hochsicheres System unsicher wird, wenn der Administrator oder auch der Benutzer ein mangelndes Sicherheitsbewusstsein hat.

Viren sind nicht mit Würmern zu verwechseln, die Phänomene auch der Netzwerksicherheit sind und keinen Wirt brauchen, um sich zu verbreiten.

Netzwerksicherheit

Bei der lokalen Sicherheit war es die Aufgabe, die Benutzer, die an demselben Rechner arbeiten, voneinander zu trennen, insbesondere den Benutzer `'root'`. Im Gegensatz dazu soll bei der Netzwerksicherheit das ganze System gegen Angriffe über das Netzwerk geschützt werden. Benutzerauthentifizierung beim klassischen Einloggen durch Benutzerkennung und Passwort gehört zur lokalen Sicherheit. Beim Einloggen über eine Netzwerkverbindung muss man differenzieren zwischen beiden Sicherheitsaspekten: bis zur erfolgten Authentifizierung spricht man von Netzwerksicherheit, nach dem Login geht es um lokale Sicherheit.

X-Windows (X11-Authentifizierung)

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X11, dem Windowing-System von Unix, gilt dies in besonderem Maße! Sie können sich ohne Weiteres auf einem entfernten Rechner einloggen und dort ein Programm starten, welches dann über das Netzwerk

auf Ihrem Rechner angezeigt wird. Das Protokoll, welches zwischen der X-Applikation und dem X-Server (der lokale Prozess, der die Fenster auf der Grafikkarte zur Anzeige bringt) zur Kommunikation verwendet wird, ist recht sparsam, was Netzwerkbandbreiten angeht. Das ist durch die in den 80er Jahren, als das System entworfen wurde, zur Verfügung stehenden Bandbreiten bedingt.

Wenn nun ein X-Client über das Netzwerk bei unserem X-Server angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (das Display), gegen unberechtigte Zugriffe schützen. Konkret heißt das hier, dass das Client-Programm Rechte bekommen muss. Bei X-Windows geschieht dies auf zwei verschiedene Arten: Host-basierte und cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Rechners, auf dem das Client-Programm laufen soll und wird mit dem Programm `xhost` kontrolliert. Das Programm `xhost` trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank im X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Es könnte noch ein zweiter Benutzer auf dem Rechner mit dem Client-Programm aktiv sein, und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server. Deswegen soll hier auch nicht näher auf diese Methoden eingegangen werden. Die Manpage des **`xhost`**-Kommandos gibt mehr Aufschluss über die Funktionsweise (und enthält ebenfalls die Warnung!).

Bei „cookie“-basierter Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der legitim eingeloggte Benutzer kennen, als einem Passwort ähnliches Ausweismittel verwendet. Dieses „cookie“ (das englische Wort cookie bedeutet Keks und meint hier die chinesischen fortune cookies, die einen Spruch enthalten) wird in der Datei `.Xauthority` im home-Verzeichnis des Benutzers beim login abgespeichert und steht somit jedem X-Windows-client, der ein Fenster beim X-Server zur Anzeige bringen will, zur Verfügung. Das Programm `xauth` gibt dem Benutzer das Werkzeug, die Datei `.Xauthority` zu untersuchen. Wenn Sie `.Xauthority` aus Ihrem home-Verzeichnis löschen oder umbenennen, dann können Sie keine weiteren Fenster von neuen X-Clients mehr öffnen. Näheres über Sicherheitsaspekte von X-Windows erfahren Sie in der manpage von `Xsecurity` (**`man Xsecurity`**).

`ssh` (secure shell) kann über eine vollständig verschlüsselte Netzverbindung für einen Benutzer transparent (also nicht direkt sichtbar) die Verbindung zu einem X-Server weiterleiten. Man spricht von „X11-forwarding“. Dabei wird auf der Server-Seite ein X-Server simuliert und bei der Shell auf der remote-Seite die DISPLAY-Variable gesetzt. Der Client öffnet zum Anzeigen dann eine Verbindung zum sshd (secure shell daemon, das serverseitige Programm), der dann die Verbindung an den richtigen, realen X-Server durchschleust. Wenn Sie X-Clients über das Netzwerk anzeigen lassen müssen, dann sollten Sie `ssh` einmal genauer unter die Lupe nehmen. Die manpage von `ssh` gibt weitere Auskünfte über diese Funktionalität.

Achtung

Wenn Sie den Rechner, auf dem Sie sich einloggen, nicht als sicher betrachten, dann sollten Sie auch keine X-Windows-Verbindungen weiterleiten lassen. Mit eingeschaltetem „X11-forwarding“ könnten sich auch Angreifer über Ihre ssh-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatur belauschen.

Weiter Informationen zu `ssh` finden Sie im Abschnitt C.1 auf Seite 153 dieses Buches.

Buffer Overflows und Format String Bugs

Nicht direkt klassifizierbar in lokal und remote gilt das im Abschnitt „Lokale Sicherheit“ über „Buffer Overflows“ und „Format String Bugs“ Gesagte äquivalent für Netzwerksicherheit. Wie auch bei den lokalen Varianten dieser Programmierfehler führen Buffer Overflows bei Netzwerkdiensten meistens zu `'root'`-Rechten. Sollte dies nicht der Fall sein, dann könnte sich der Angreifer zumindest Zugang zu einem unpriviligierten lokalen Account verschaffen, mit dem er dann weitere (lokale) Sicherheitsprobleme ausnutzen kann, falls diese vorhanden sind.

Über das Netzwerk ausbeutbare Buffer Overflows und Format String Bugs sind wohl die häufigsten Varianten von remote-Angriffen überhaupt. Auf Sicherheitsmailinglisten werden so genannte „exploits“ herumgereicht, d.h. Programme, die die frisch gefundenen Lücken ausnutzen. Auch jemand, der nicht die genauen Details der Lücke kennt, kann damit die Lücke ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von „exploitcodes“ generell die Sicherheit von Betriebssystemen erhöht hat, was sicherlich daran liegt, dass Betriebssystemhersteller dazu gezwungen waren, die Probleme in ihrer Software zu beseitigen. Da bei freier Software der Sourcecode für jedermann erhältlich ist (SuSE-Linux liefert alle verfügbaren Quellen mit), kann jemand, der eine Lücke mitsamt „exploitcode“ findet, auch gleichzeitig noch einen Reparaturvorschlag für das Problem anbieten.

DoS — Denial of Service

Ziel dieser Art von Angriff ist das Einstellen des Dienstes (oder gleich des ganzen Systems). Dies kann auf verschiedenste Arten passieren: Durch Überlastung, durch Beschäftigung mit unsinnigen Paketen oder durch Ausnutzen von „Remote Buffer Overflows“, die nicht direkt zum Ausführen von Programmen auf der remote-Seite ausbeutbar sind.

Der Zweck eines DoS mag meistens darin begründet sein, dass der Dienst einfach nicht mehr verfügbar ist. Dass ein Dienst fehlt, kann aber weitere Konsequenzen haben. Siehe „man in the middle: sniffing, tcp connection hijacking, spoofing“ und „DNS poisoning“.

man in the middle: sniffing, tcp connection hijacking, spoofing

Ganz allgemein gilt: Ein Angriff vom Netzwerk, bei der der Angreifer eine Position zwischen zwei Kommunikationspartnern einnimmt, nennt sich „man in the middle attack“. Sie haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar: Der Angreifer nimmt die Verbindung entgegen und stellt, damit das Opfer nichts merkt, selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Rechner geöffnet, weil dieser sich als das Ziel ausgibt. Der einfachste „man in the middle attack“ ist ein „sniffer“. Er belauscht einfach nur die Netzverbindungen, die an ihm vorüber geführt werden (sniffing = engl. schnüffeln). Komplexer wird es, wenn der Angreifer in der Mitte versucht, eine etablierte, bestehende Verbindung zu übernehmen (entführen = engl. hijacking). Dafür muss der Angreifer die Pakete, die an ihm vorbeigeführt werden, eine Weile lang analysiert haben, damit er die richtigen TCP-Sequenznummern der TCP-Verbindung vorhersagen kann. Wenn er dann die Rolle des Ziels der Verbindung übernimmt, merkt das das Opfer, weil auf der Seite des Opfers die Verbindung als ungültig terminiert wird.

Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen „hijacking“ gesichert sind und bei denen zu Beginn der Verbindung einen Authentifizierung stattfindet. „Spoofing“ nennt sich das Verschicken von Paketen mit modifizierten Absenderdaten, also hauptsächlich der IP Adresse. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`'root'`) darf.

Viele der Angriffsmöglichkeiten kommen in Kombination mit einem DoS vor. Gibt es eine Möglichkeit, einen Rechner schlagartig vom Netzwerk zu trennen (wenn auch nur für kurze Zeit), dann wirkt sich das förderlich auf einen aktiven Angriff aus, weil keine Störungen mehr erwartet werden müssen.

DNS poisoning

Der Angreifer versucht, mit gefälschten („gespooften“) DNS-Antwortpaketen den cache eines DNS-Servers zu vergiften (engl. *poisoning*), so dass dieser die gewünschte Information an ein Opfer weitergibt, das danach fragt. Um einem DNS-Server solche falschen Informationen glaubhaft zuschieben zu können, muss der Angreifer normalerweise einige Pakete des Servers bekommen und analysieren. Weil viele Server ein Vertrauensverhältnis zu anderen Rechnern aufgrund ihrer IP Adresse oder ihres Hostnamens konfiguriert haben, kann ein solcher Angriff trotz eines gehörigen Aufwands recht schnell Früchte tragen. Voraussetzung ist allerdings eine gute Kenntnis der Vertrauensstruktur zwischen diesen Rechnern. Ein zeitlich genau abgestimmter DoS gegen einen DNS-Server, dessen Daten gefälscht werden sollen, ist aus Sicht des Angreifers meistens nicht vermeidbar.

Abhilfe schafft wieder eine kryptographisch verschlüsselte Verbindung, die die Identität des Ziels der Verbindung verifizieren kann.

Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied: Ein Wurm muss keinerlei Wirtsprogramm infizieren, und er ist darauf spezialisiert, sich möglichst schnell im Netzwerk zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen wohlbekannte Sicherheitslücken von Serverprogrammen wie `bind8` oder `lprNG`. Man kann sich relativ einfach gegen Würmer schützen, weil zwischen dem Zeitpunkt des Bekanntwerdens der ausgenutzten Lücken bis zum Auftauchen des Wurms normalerweise einige Tage vergehen, so dass update-Pakete vorhanden sind. Natürlich setzt dies voraus, dass der Administrator die Security-updates auch in seine Systeme einspielt.

C.2.3 Tipps und Tricks: Allgemeine Hinweise

Information: Für einen effizienten Umgang mit dem Bereich Sicherheit ist es nötig, mit den Entwicklungen Schritt zu halten und auf dem Laufenden zu sein, was die neuesten Sicherheitsprobleme angeht. Ein sehr guter Schutz gegen Fehler aller Art ist das schnellstmögliche Einspielen von update-Paketen, die von einem Security-Announcement angekündigt werden. Die SuSE-security-Announcements werden über eine Mailingliste verbreitet, in die Sie sich, den Links unter `http://www.suse.de/security` folgend, eintragen können.

`suse-security-announce@suse.de` ist die erste Informationsquelle für update-Pakete, die vom Security-Team mit neuen Informationen beliefert wird.

Die Mailingliste `suse-security@suse.de` ist ein lehrreiches Diskussionsforum für den Bereich Sicherheit. Sie können sich auf der gleichen URL wie für `suse-security-announce@suse.de` für die Liste anmelden.

Eine der bekanntesten Sicherheitsmailinglisten der Welt ist die Liste `bugtraq@securityfocus.com`. Die Lektüre dieser Liste bei durchschnittlich 15-20 Postings am Tag kann mit gutem Gewissen empfohlen werden. Mehr Information finden Sie auf `http://www.securityfocus.com`.

Einige Grundregeln, die zu kennen nützlich sein kann, sind nachstehend aufgeführt:

- Vermeiden Sie es, als `'root'` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu benutzen. Das verringert die Chancen für ein Kukuksei oder einen Virus, und überdies für Fehler Ihrerseits.
- Benutzen Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten remote auszuführen. „ssh“ (secure shell) ist Standard, vermeiden Sie `telnet`, `ftp`, `rsh` und `rlogin`.
- Benutzen Sie keine Authentifizierungsmethoden, die alleine auf der IP-Adresse aufgebaut sind.
- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die Mailinglisten für Announcements der jeweiligen Software (z. B. Beispiel `bind`, `sendmail`, `ssh`). Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.

- Optimieren Sie die Zugriffsrechte auf sicherheitskritische Dateien im System, indem Sie die `/etc/permissions`-Datei Ihrer Wahl an Ihre Bedürfnisse anpassen. Ein setuid-Programm, welches kein setuid-bit mehr hat, mag zwar nicht mehr wirklich seine Aufgabe erledigen können, aber es ist in der Regel kein Sicherheitsproblem mehr. Mit einer ähnlichen Vorgehensweise können Sie auf welt-schreibbare Dateien und Verzeichnisse losgehen.

- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer, und es verhindert, dass Ihre Benutzer sich an einen Dienst gewöhnen, den Sie nie absichtlich freigegeben haben (legacy-Problem). Offene Ports (mit socket-Zustand LISTEN) finden Sie mit dem Programm `netstat`. Verwenden Sie **`netstat -ap`** oder **`netstat -anp`** als Optionen. Mit der **`-p`**-Option können Sie gleich sehen, welcher Prozess mit welchem Namen den Port belegt.

  Vergleichen Sie die Ergebnisse, die Sie haben, mit einem vollständigen Portscan Ihres Rechners von außen. Das Programm `nmap` ist dafür hervorragend geeignet. Es klopft jeden einzelnen Port ab und kann anhand der Antwort Ihres Rechners Schlüsse über einen hinter dem Port wartenden Dienst ziehen. Scannen Sie niemals einen Rechner ohne das direkte Einverständnis des Administrators, denn dies könnte als aggressiver Akt aufgefasst werden. Denken Sie daran, dass Sie nicht nur TCP-Ports scannen sollten, sondern auf jeden Fall auch UDP-Ports (Optionen **`-sS`** und **`-sU`**).

- Zur zuverlässigen Integritätsprüfung der Dateien in Ihrem System sollten Sie `tripwire` benutzen und die Datenbank verschlüsseln, um sie gegen manipulative Zugriffe zu schützen. Darüber hinaus brauchen Sie auf jeden Fall ein backup dieser Datenbank außerhalb der Maschine auf einem eigenen Datenträger, der nicht über einen Rechner mit einem Netzwerk verbunden ist.

- Seien Sie vorsichtig beim Installieren von Fremdsoftware. Es gab schon Fälle, wo ein Angreifer tar-Archive einer Sicherheitssoftware mit einem trojanischen Pferd versehen hat. Zum Glück wurde dies schnell bemerkt. Wenn Sie ein binäres Paket installieren, sollten Sie sicher sein, woher das Paket kommt.

  SuSE rpm-Pakete werden gpg-signiert ausgeliefert. Der Schlüssel, den wir zum Signieren verwenden, ist

  ID:9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>

  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA

  Das Kommando **`rpm -checksig paket.rpm`** zeigt an, ob die Prüfsumme und die Signatur des (nicht installierten!) Pakets stimmen. Sie finden den Schlüssel auf der ersten CD einer SuSE-Distribution ab SuSE-7.1 und auf den meisten Keyservern der Welt.

- Überprüfen Sie regelmäßig Ihr Backup der Daten und des Systems. Ohne eine zuverlässige Aussage über die Funktion des Backups ist das Backup unter Umständen wertlos.

- Überwachen Sie Ihre „Logfiles“. Nach Möglichkeit sollten Sie sich ein kleines Script schreiben, welches Ihre Logfiles nach ungewöhnlichen Einträgen

absucht. Diese Aufgabe ist alles andere als trivial, denn nur Sie wissen, was ungewöhnlich ist und was nicht.

- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Rechners auf die IP-Adressen einzuschränken, denen der Zugriff auf einen bestimmten Dienst explizit gestattet ist. Nähere Information zu den `tcp_wrappern` finden Sie in der manual page von `tcpd(8)` und `hosts\_access` (**`man tcpd`**, **`man hosts_access`**).
- Legen Sie Ihr Sicherheitsdenken redundant aus: Eine Meldung, die zweimal eintrifft, ist besser als eine, die Sie nie sehen. Dies gilt genauso für Gespräche mit Kollegen.

C.2.4 Zentrale Meldung von neuen Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie die zur Verfügung stehenden update-Pakete), dann wenden Sie sich bitte vertrauensvoll an die E-Mail-Adresse `security@suse.de`. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. Wir werden uns bemühen, Ihnen so schnell wie möglich zu antworten. Eine pgp Verschlüsselung Ihrer E-Mail ist erwünscht. Unser pgp key ist:

ID:3D25D3D9 1999-03-06 SuSE Security Team <security@suse.de>

Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5

Der Schlüssel liegt auch unter `http://www.suse.de/security` zum Download bereit.

D YaST und SuSE Linux Lizenzbestimmungen

YaST – Copyright (c) 1995-2001 SuSE GmbH, Nürnberg (Germany)

Gegenstand dieser Lizenz ist das Programm YaST (engl. *Yet another Setup Tool*), der Name „YaST“, sowie SuSE Linux, die Linux-Distribution der SuSE GmbH, alle aus YaST abgeleiteten Programme und auf YaST vollständig oder auszugsweise abgeleiteten Werke oder Namen *und jedes andere unter dieser Lizenz stehende Programm der SuSE GmbH*, sowie die Benutzung, Verwendung, Archivierung, Vervielfältigung und Weitergabe der *unter dieser Lizenz stehenden Programme*, aller aus *unter dieser Lizenz stehenden Programme* abgeleiteten Programme und alle vollständig oder auszugsweise abgeleiteten Werke hiervon. *Die unter dieser Lizenz stehenden Programme* mit allen Quellen sind im Sinne des Urheberrechts geistiges Eigentum der SuSE GmbH. Der Name YaST ist ein eingetragenes Warenzeichen der SuSE GmbH. Im folgenden tritt die SuSE GmbH als Lizenzgeber auf, und jeder Benutzer oder Bearbeiter *unter dieser Lizenz stehender Programme der SuSE GmbH*, daraus vollständig oder auszugsweise abgeleiteter Werke sowie jede Person, die YaST, *andere unter dieser Lizenz stehende Programme der SuSE GmbH* oder SuSE Linux archiviert, vervielfältigt und verbreitet, ist Lizenznehmer der SuSE GmbH.

Durch die Bearbeitung, Benutzung, Verwendung, Archivierung, Vervielfältigung und Weitergabe von YaST *oder eines anderen unter dieser Lizenz stehenden Programmes der SuSE GmbH* werden die folgenden Lizenzbestimmungen anerkannt.

Nur diese Lizenz gibt dem Lizenznehmer das Recht, YaST, daraus abgeleitete Werke sowie *alle anderen unter dieser Lizenz stehenden Programme bzw. daraus abgeleitet Werke* der SuSE GmbH zu benutzen, zu vervielfältigen, zu verteilen oder zu verändern. Diese Handlungen sind durch das Urheberrecht untersagt, wenn diese Lizenz nicht anerkannt wird. Wird diese Lizenz im ganzen anerkannt und befolgt, ist sie auch ohne schriftliche Zustimmung des Lizenznehmers gültig.

1. Benutzung

   YaST, SuSE Linux und *alle anderen unter dieser Lizenz stehenden Programme der SuSE GmbH* dürfen für private und kommerzielle Zwecke unter Beachtung der Urheberrechte und Lizenzbestimmungen der installierten Pakete und Programme genutzt werden. Die Benutzung von YaST oder *anderer unter dieser Lizenz stehender Programme*, auch bei Verwendung einer modifizierten Version, befreit insbesondere den Lizenznehmer NICHT von der gebotenen Sorgfaltspflicht gegenüber den Lizenzbestimmungen der durch

YaST und *aller anderen unter dieser Lizenze stehenden Programme* oder darauf basierenden Werken installierten Pakete und Programme.

2. Bearbeitung

   Alle aus YaST oder *anderen unter dieser Lizenz stehenden Programme oder abgeleiteten Programme* und alle vollständig oder auszugsweise abgeleiteten Werke *hieraus* sind auf dem Eröffnungsbildschirm mit dem eindeutigen Hinweis „Modifizierte Version“ zu versehen. Desweiteren hat der Bearbeiter seinen Namen, einen Hinweis, dass die SuSE GmbH für die „Modifizierte Version“ keinen Support leistet und den Ausschluss jedweder Haftung auf dem Eröffnungsbildschirm anzugeben. Als „Modifizierte Version“ gilt jede Änderung in den Quellen, die nicht von der SuSE GmbH durchgeführt wird. Der Lizenznehmer hat das Recht, seine Kopie der Quellen von YaST und *aller anderen unter dieser Lizenz stehenden Programme* zu verändern, wodurch ein auf dem entsprechenden Programm basierendes Werk entsteht, vorausgesetzt, dass die folgenden Bedingungen erfüllt sind:

   a) Jede Änderung muss in den Quellen mit Datum und Bearbeiter vermerkt sein. Die veränderten Quellen müssen nach Abschnitt 3), zusammen mit dieser unveränderten Lizenz, dem Benutzer zu Verfügung gestellt werden.

   b) Der Lizenznehmer ist verpflichtet, dass jede von ihm verbreitete Arbeit, die ganz oder teilweise von YaST oder *einem anderen unter dieser Lizenz stehenden Programm* oder Teilen hiervon abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.

   c) Die Änderung dieser Lizenz durch einen Lizenznehmer, auch nur teilweise, ist untersagt.

   Die SuSE GmbH behält sich das Recht vor, unentgeltlich Teile oder alle Änderungen einer modifizierten Version von YaST *oder eines anderen unter dieser Lizenz stehenden Programms* in die offizielle Version *des jeweiligen Programms aufzunehmen*. Der Lizenznehmer hat darauf keinen Einfluss.

3. Weitergabe

   Es ist untersagt, ohne vorherige schriftliche Genehmigung der SuSE GmbH YaST, SuSE Linux oder *ein anderes unter dieser Lizenz stehendes Programm* gegen Entgelt zu vervielfältigen oder unberechtigt vervielfältigte Datenträger zu verbreiten. Die Verteilung gegen Entgelt des Programms YaST oder *eines anderen unter dieser Lizenz stehenden Programms*, dessen Quellen, ob vollständig oder teilweise verändert oder unverändert, und der daraus abgeleiteten Werke bedürfen der vorherigen schriftlichen Zustimmung der SuSE GmbH.

   Alle aus YaST oder *einem anderen unter dieser Lizenz stehenden Programms*, abgeleiteten Programme und alle vollständig oder auszugsweise abgeleiteten Werke dürfen nach 2b) nur mit den veränderten Quellen und dieser Lizenz weitergegeben werden. Die kostenfreie Bereitstellung von YaST, *aller anderen unter dieser Lizenz stehenden Programme* oder daraus abgeleiteter Werke zusammen mit SuSE Linux auf FTP-Servern und Mailboxen ist unter Beachtung der Lizenzen der Software gestattet.

4. Gewährleistung

   Für YaST, SuSE Linux und *andere unter dieser Lizenz stehenden Werke* oder daraus abgeleitete Werke und SuSE Linux ist jegliche Gewährleistung ausgeschlossen. Die Gewährleistung der SuSE GmbH erstreckt sich nur auf fehlerfreie Datenträger.

   Die SuSE GmbH stellt YaST, SuSE Linux und *jedes andere unter dieser Lizenz stehende Programm* so zur Verfügung, *WIE ES IST*, ohne jedwede Gewährleistung, ohne die Tauglichkeit für einen bestimmten Zweck oder die Verwendbarkeit zu garantieren. Insbesondere haftet SuSE nicht für entgangenen Gewinn, ausgebliebene Einsparungen oder Schäden aus Ansprüchen Dritter gegenüber dem Lizenznehmer. Die SuSE GmbH haftet auch nicht für sonstige mittelbare oder unmittelbare Folgeschäden, insbesondere nicht für den Verlust oder die Erstellung aufgezeichneter Daten.

   Die Beachtung der jeweiligen Lizenzen und Urheberrechte der installierten Software obliegt allein dem Benutzer von YaST, SuSE Linux oder *einem anderen unter Lizenz stehenden Programms*.

5. Rechte

   Es werden keine weiteren Rechte an YaST, SuSE Linux und *allen anderen unter dieser Lizenz stehenden Programme* als die in dieser Lizenz behandelten eingeräumt. Ein Verstoß gegen diese Lizenz beendet automatisch die Rechte des Lizenznehmers. Jedoch werden die Rechte Dritter, die vom Lizenznehmer Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese Lizenz in allen Teilen anerkannt und befolgt wird. Falls der Lizenznehmer aufgrund eines Gerichtsurteils, Patentbestimmungen, Lizenzbestimmungen oder aus einem anderen Grund Bedingungen oder Verpflichtungen auferlegt werden, die dieser Lizenz ganz oder in Teilen widersprechen, so wird der Lizenznehmer ausdrücklich nur mit vorheriger schriftlicher Zustimmung der SuSE GmbH von dieser Lizenz und ihren Bedingungen ganz oder teilweise befreit. Es ist das Recht der SuSE GmbH, diese Zustimmung ohne Angabe von Gründen zu verweigern.

6. Weitere Einschränkungen

   Wenn die Verbreitung oder Benutzung von YaST, *eines anderen unter dieser Lizenz stehenden Programmes*, SuSE Linux oder Teilen von SuSE Linux in einem Staat entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann die SuSE GmbH eine explizite geographische Begrenzung der Verbreitung *des betroffenen Programmes* angeben, mit der diese Staaten ganz oder teilweise von der Verbreitung ausgeschlossen werden. In einem solchen Fall beinhaltet diese Lizenz die ganze oder teilweise Beschränkung, als wäre sie in dieser Lizenz niedergeschrieben.

Index