HTWK Leipzig
Fachbereich IMN
Wintersemester 2012/2013

# Die Möglichkeiten des System-Managements der Firewall-Distribution pfSense –VORABVERSION–

Beleg im Fach Netzwerk- und System-Management

VORABVERSION

Marcel Kirbst
Sieglitz 39
06618 Molau
marcel.kirbst@stud.htwk-leipzig.de
21. Februar 2013

# Inhaltsverzeichnis



VORABVERSION

# Abbildungsverzeichnis



VORABVERSION

# 1 Einleitung

Dieser Beleg befasst sich der Vorstellung der Routerdistribution pfSense. Im Vergleich zu den unzähligen anderen, existierenden Routerdistributionen zeichnet sich pfSense durch seinen hohen Funktionsumfang aus, der beispielsweise auch Funktionen zur Sicherstellung von Redundanz und Ausfallsicherheit umfasst, wie sie sonst nur bei preisintensiven proprietären Lösungen kommerzieller Anbieter verfügbar sind.
Nachdem grundlegende Begriffe erläutert wurden, soll kurz auf die Entwicklungsgeschichte und Vorzüge des Betriebssystems FreeBSD eingegangen werden, welches die Grundlage für pfSense bildet. Im folgenden soll ein kurzer Überblick über den Funktionsumfang von pfSense gegeben werden, für sich genommen und im Vergleich zu anderen Rouuterdistributionen. Abschließend sollen beispielhaft drei Konfigurationen vorgestellt werden um die Vielseitigkeit und Leistungsfähigkeit von pfSense zu demonstrieren.

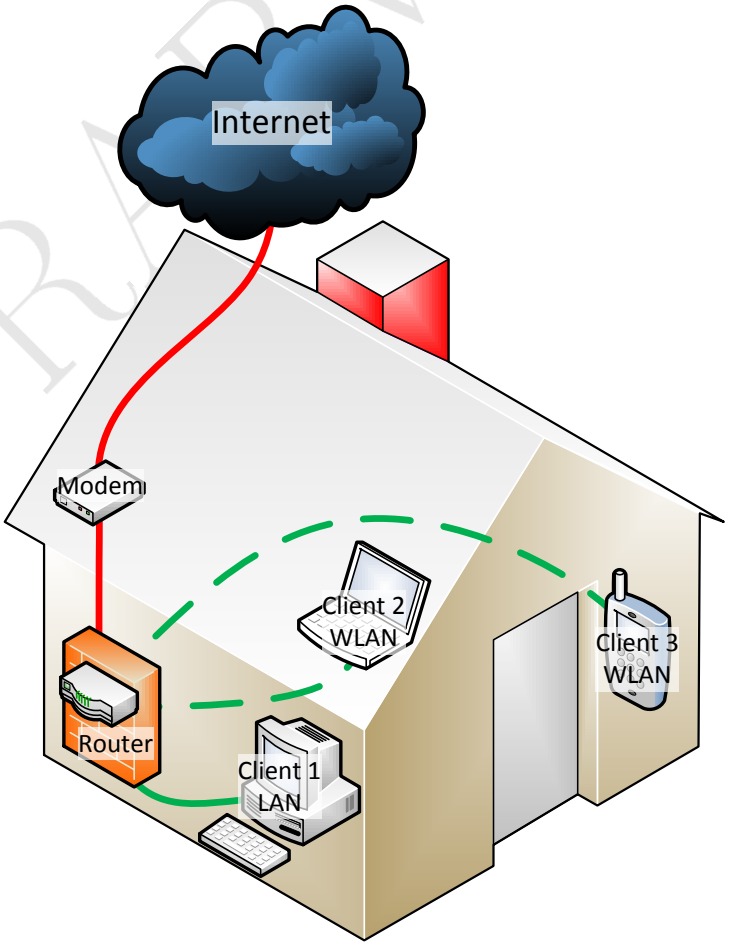


Abbildung 1: Beispielhafte Standardkonfiguration eines Internetanschluß.

VORABVERSION

# 2 Routerdistributionen - Besonderheiten und Merkmale im Allgemeinen

## 2.1 Begrifflichkeiten im Zusammenhang mit Routerdistributionen

Routerdistributionen sind auf einen speziellen Einsatzzweck hin optimierte Betriebssysteme.
Unter dem Begriff Betriebssystem fasst man eine Menge von Software zusammen, die auf einem Rechnersystem nach dem Start zur Ausführung kommt, die Ressourcen dieses Rechnersystems verwaltet und es ermöglicht weitere Anwenungsprogramme zu starten.
Routerdistributionen werden in der Regel so konzipiert und entwickelt, um direkt auf einem Rechnersystem installiert zu werden und über alle Ressourcen dieses Rechnersystems zu verfügen. Dieser Annahme kommt eine besonders hohe Bedeutung zu, da die beiden Schwerpunkte einer Routerdistribution Sicherheit und Stabilität darstellen. Andere Merkmale wie zum Beispiel möglichst hoher Funktionsumfang besitzen dem gegenüber niedrigere Priorität, wobei jedoch verschiedene Routerdistributionen die einzelnen Merkmale im Detail unterschiedlich stark priorisieren.
Ein Router ist ein Netzwerkgerät, das mit mindestens zwei Netzwerkschnittstellen ausgestattet ist und den Netzwerkverkehr zwischen den betreffenden Netzwerken, unter Beachtung eines vorgegebenen Regelwerkes, vermittelt.

## 2.2 Merkmale von Routerdistributionen

Routerdistributionen werden in der Regel nicht von Grund auf entwickelt sondern basieren auf einem modifizierten Betriebssystem. Trotz dieser Modifikationen unterliegen die verschiedenen Routerdistributionen somit mehr oder weniger stark den Merkmalen, Besonderheiten und Einschränkungen des jeweils zu Grunde liegenden Betriebssystems. Somit ist das zu Grunde liegende Betreibssystem ein erstes wichtiges Unterscheidungskriterium für Routerdistributionen.
Ein weiteres wichtiges Unterscheidungskriterium stellt die Art der Entwicklung und Lizenzierung dar. Es existieren kommerzielle Produkte genauso wie quelloffene Produkte. Da kommerzielle Produkte in den allermeisten Fälle jedoch nicht im Quellcode verfügbar und somit schwer an spezielle Bedürfnisse anzupassen sind und außerdem oft beträchtliche Lizenzkosten verursachen, soll dieser Typus von Routerdistributionen in dieser Arbeit außen vor bleiben.

VORABVERSION

Weiterhin spielt für den potentiellen Einsatz im kommerziellen Umfeld neben Funktionen wie zum Beispiel VLAN-Unterstützung auch der Faktor der Verfügbarkeit eines kommerziellen Supports eine wichtige Rolle. Steht für komplexe Netzwerke wie etwa in Hochschulen oder mittelständischen und großen Unternehmen mit hunderten bis tausenden Nutzern die Konzeption und Implementierung einer Router- und Firewalllösung bevor, ist es in der Regel obligatorisch, gegebenenfalls auf schnellen kommerziellen Support zurückgreifen zu können.
Um den generellen Kostenrahmen abschätzen zu können und damit Planungssicherheit in einem bestimmten Rahmen zu bieten, sollte außerdem eine Bedarfsanalyse durchgeführt werden. Diese sollte nicht nur die derzeitigen Anforderungen berücksichtigen, sondern auch zukünftige Anforderungen, wie zum Beispiel die vollständige Unterstützung der Prtokollsammlung IPv6.
Außerdem sollen die Routerdistributionen im Bezug auf modulare Erweiterbarkeit betrachtet werden, denn bei Verfügbarkeit speziell vorgefertigter Softwarepakete, oft auch als so genannte Addons bezeichnet werden lässt sich der Nutzen der Routerdistribution für den Adminsitrator oft erheblich steigern. Jedoch soll an dieser Stelle ausdrücklich darauf hingewiesen werden, dass jeder zusätzliche Dienst auch zusätzliche potentielle Sicherheitslücken birkt. Es gilt also im Bezug auf zusätzliche Dienste bei Routerdistributionen und Firewalls der Grundsatz: “So viel wie nötig, jedoch so wenig wie möglich!”

## 2.3 Konkrete Routerdistributionen im Vergleich

Im Folgenden soll ein Vergleich dreier verbreiteter OpenSource- Routerdistributionen erfolgen.

### 2.3.1 Die Routerdistribution IPCop

IPCop ist eine Router-Distribution, die auf dem Betriebssystemkern Linux basiert und in der Version 1.0 bereits am 1. Januar 2002 veröffentlicht wurde. [1]
Nach Aussagen der Entwickler von IPCop ist die Entwicklung vor allem auf eine zuverlässige, sichere und stabile Routerdistribution hin ausgerichtet, die auch von Laien eingerichtet und betrieben werden kann. Nach der Installation lassen sich sämtliche Konfigurationsparamter über eine Weboberfläche modifizieren, ein Zugriff auf die Kommandozeile der Routerdistribution ist also im Normalfall nicht erforderlich, jedoch möglich.
Eine Erweiterbarkeit um viele Funktionen, die zu Lasten der Sicherheit geht, steht

[1] [1]

VORABVERSION

dagegen hinten an. Als Beispiel sei an dieser Stelle das Samba-Addon für IPCop erwähnt, das es ermöglichte IPCop um einen Samba-Server zu erweitern, um den Rechner im lokalen Netzwerk hinter der IPCop einen Dateiserver hauptsächlich für Windows-Clients zu bieten. Dieses Addon wurde absichtlich nicht mehr verfügbar gemacht um die Sicherheit der IPCop-Firewall nicht durch diesen zusätzlichen Dienst herabzusetzen.[2]
Mit dem Erscheinen von IPCop Version 2.0 im Jahr unterstützt IPCop weitere Hardware-Architekturen wie PowerPC, Cobalt und Sparc. Außerdem erfolgte mit Einführung von Version 2.0 eine Überarbeitung verschiedener Dienste wie zum Beispiel des Zeitservers und des DHCP-Servers[3]
Es lässt sich also sagen, dass IPCop eine Routerdistribution ist, die sich nicht durch möglichst hochgradigen Funktionsumfang sondern durch Sicherheit und Stabilität definiert.

### 2.3.2 Die Routerdistribution IPFire

IPFire basiert wie pfSense auf dem Betriebssystemkern Linux. Im Vergleich zu IPCop versucht man jedoch bei IPFire mehr Modularität zu bieten, indem für viele populäre Dienste wie Asterisk, eine Telefonserver-Software oder Samba, vorkonfigurierte Pakete zur Verfügung stehen.
Weiterhin existieren auf der offiziellen Webpräsenz auch Anleitungen um Instanzen von IPFire in einer virtuellen Umgebung wie zum Beispiel unter Xen zur Ausführung zu bringen.[4] Die Virtualisierung von Firewalls ist jedoch ein eigenes, umstrittenes Gebiet, dass in dieser Arbeit nicht weiter aufgegriffen werden soll. Es wird auf entsprechende Literatur verwiesen. (QUELLEN EINFÜGEN !!)
Im Bezug auf IPFire ist festzuhalten, dass diese wie auch IPCop auf Linux basiert, jedoch im Vergleich zu IPCop mehr versucht einen Kompromiss zwischen Sicherheit und Erweiterbarkeit zu bieten.

### 2.3.3 Die Routerdistribution pfSense

Die Routerdistribution pfSense basiert auf dem Betriebssystem FreeBSD. Wie die anderen vorgestellen Routerdistributionen lässt sich auch pfSense nach der Installation quasi vollständig über die Weboberfläche administrieren.
Da pfSense auf FreeBSD aufbaut, ist diese Routerdistribution auch den gleichen Vorzügen und Nachteilen unterworfen wie FreeBSD.

[2] [2]
[3] [3]
[4] [4]

VORABVERSION

Die Hardwareunterstützung von FreeBSD ist nicht so umfangreich wie beispielsweise für Linux. Das sollte bei der Anschaffung von neuer Hardware für Routerdistributionen beachtet werden.[5] Im Gegenzug bietet FreeBSD von Haus aus schon enorme Vorteile im Bezug auf den Funktionsumfang, beispielsweise war FreeBSD eines der ersten Betriebssystem die den IPv6-Stack vollständig implementierten. Weitere Funktionen sind die Unterstützung von virtuellen Netzwerken, so genannten VLAN's, beim Einsatz geeigneter Netzwerkkarten sowie Implementierung von Techniken Wie CARP und XMLRPC, die Vorraussetzung sind, wenn redundante Router- und Firewallcluster implementiert werden sollen.
Weiterhin existiert für pfSense ein eigenes Paketverwaltungssystem, welches direkt aus der Weboberfläche erreichbar ist und welches pfSense um weitere Dienste und Funktionen erweitern kann. Es folgt eine Auflistung einer Auswahl von Paketen:

**asterisk** verbreiteter Telefonserver-Dienst

**country block** erlaubt das Blockieren von eingehendem Internetverkehr anhand dessen länderspezifischer Herkunft

**freeradius** freie Implementierung eines Radius-Servers der es ermöglicht, die Benutzer sämtlicher Dienste im Netzwerk gegen diesen Dienst authentifizieren zu lassen, beispielsweise Dateiserver oder WLAN-Zugang auf Basis von WPA(2)-Enterprise.

**squid** leistungsfähiger Proxy-Server.

Durch den hohen Funktionsumfang der auch Techniken zur Realisierung von Hochverfügbarkeitsclustern und der logischen Segmentierung des lokalen Netzwerks umfasst ist pfSense für den Einsatz in mittleren bis großen Netzwerken, wie sie in Unternehmen und Hochschulen überlicherweise vorhanden sind, eine interessante Alternative zu kommerziellen Produkten. Jedoch ist auch im Privatbereich der Einsatz von pfSense als Heimrouter-Software üblich, unter anderem deshalb, weil eine übersichtliche und gut strukturiere Weboberfläche Bestandteil dieser Routerdistribution ist, die auch mehrere Assistenen beinhaltet um dem Administrator die Konfiguration zu erleichtern

### 2.3.4 Leistungsmerkmale der vorgestellten Routerdistributionen im Vergleich

Im folgenden sollen die wichtigsten Vorzüge und Leistungsmerkmale der ausgewählten Routerdistributionen noch einmal direkt gegenüber gestellt werden.

[5] [8]

VORABVERSION

Berücksichtigt werden im Folgenden jedoch nur Funktionen, die bei einer Standardinstallation bereits verfügbar sind oder durch ein eventuell vorhandes Paketmanagement für die jeweilige Routerdistribution benutzerfreundlich nachgerüstet werden können und somit die Stabilität und Sicherheit des Gesamtsystems nicht oder nur geringfügig verschlechtern. Da es sich bei allen drei Kandidaten um OpenSource-Lösungen handelt können zusätzliche Funktionen natürlich mit unterschiedlich hohem Aufand trotzdem nachgerüstet werden, jedoch handelt es sich dann um individuelle Modifikationen die in der Praxis in der Regel nicht im größeren Umfeld getestet wurden und eventuell bei späteren Updates der Firewalldistribution Konflikte verursachen.

| Funktion | **IPCop** | **IPFire** | **pfSense** |
|---|---|---|---|
| Lizenz | GPL[5] | GPL[5] | BSD[7] |
| Betriebssystem | Linux | Linux | FreeBSD |
| Hardware"-architektur | i386, Cobald, Sparc, PowerPC | i386, AMD64 | i386, AMD64 |
| vorkonfigurierte Pakete | nein | ja | ja |
| eigene Paketverwaltung | nein | nein | ja |
| Automatisches Update | nein | nein | ja |
| VLAN-Unterstützung | nein | nein | ja mit entsprechenden Netzwerkkarten |
| Netzwerkschnittstell | max. 4 | max. 4 | nur durch Hardware begrenzt |
| Redundanz bezüglich Fehlfunktionen der Hardware | Softwarebasiertes RAID1 mittels mdadm | nein[6] | Softwarebasiertes RAID 1 mittels GEOM |
| Clusterfähigkeit | nein | nein | ja, durch CARP, XMLRPC, pfsync |
| Kommerzieller Support verfügbar ? | ja | ja | ja |

[6] [9]

VORSCHAU VERSION

Tabelle 1: Merkmale ausgewählter Routerdistributionen im Vergleich

Aus dem tabellarischen Vergleich der drei Router-Distributionen ist ersichtlich, dass pfSense vom Funktionsumfang und auch im Bezug auf die Funktionalitäten im Firmenumfeld den anderen Distributionen deutlich überlegen ist. Aus diesem Grund sollen im Folgenden ein Überblick über pfSense erfolgen.

# 3 pfSense im Überblick

Die Firewall-Distribution pfSense ist eine sehr leistungsfähige Software mit hohem Funktionsumfang, welche im folgenden Kapitel vorgestellt werden soll.

## 3.1 Das Betriebssystem FreeBSD - Basis von pfSense

Die Router-Distribution pfSense basiert auf dem Betriebssystem FreeBSD. Aus diesem Grund soll in diesem Abschnitt kurz auf die Vorzüge und Besonderheiten von FreeBSD eingegangen werden. FreeBSD ist ein unixodies Betriebssytem welches eine Reihe von fortschrittlichen Techniken implementiert. Beispielhaft seien an dieser Stelle der Netzwerk-Paketfilter mit der Bezeichnung pf genannt, der duch das Tool pfsync um die Funktionalität der Netzwerksynchroniserbarkeit erweitert wird. Weiterhin implementiert FreeBSD eine Technik mit der Bezeichnung Common Address Redundancy Protokoll, welche eine Synchronisierung des Zustandes der Verbindungstabelle zwischen FreeBSD-Instanzen erlaubt. FreeBSD implementiert einen sehr robusten und leistungsfähigen Netzwerkstack, der es für den Einsatz als Betriebssystem auf Netzwerkkomponenten wie Routern und Servern prädestiniert. Beispielsweise war FreeBSD eines der ersten Betriebssysteme die im Jahr 2003 einen vollständigen IPv6-Netzwerkstack implementierten. Einen wichtigen Schwerpunkt im Design und der Entwicklung von FreeBSD spielt Sicherheit. Durch Techniken wie die so genannten BSD-Jails, die in FreeBSD seit vielen Jahren zur Verfügung stehen rechtfertigt FreeBSD seinen hervorragenden Ruf im Bezug auf die Sicherheit. Nicht zuletzt die Lizenz, unter der FreeBSD veröffentlicht wird und die dem Benutzer sehr weitreichende Rechte einräumt, ist besonders hervor zu heben.
Im Vergleich zu anderen verbreiteten BSD-Dreviaten wie OpenBSD bietet FreeBSD außerdem über das so genannte Port-System Zugriff auf eine umfangreiche Auswahl von Software aus der Linux-Welt.
Als weiterführende Literatur sei auf [1] und [2] sowie die Online-Dokumentation[7] zu

[7] [6]

VORABVERSION

FreeBSD verwiesen.

## 3.2 pfSense Features

[12] - pfSense bis Version 2.0 hauptsächlich Weboberfläche für FreeBSD - komplette Konfiguration in einer einzigen XML-Datei - ab 2.1 voller IPv6-Support - kommerzieller Support verfügbar - 802.11q VLAN Support - DHCP-Server - SNMP - Sicherung und Wiederherstellung der Konfiguration per Web-Oberfläche - Verwendung von Alias-Bezeichnern für einzelne Rechner und Gruppen - Load Balancing für eingehenden und ausgehenden Netzwerkverkehr - Unterstützung für mehrere WAN-Anschlüsse gleichzeitig - optimiert auf möglichst wenig Neustarts nach Änderungen an der Konfiguration - - Anwendungsfälle

VORABVERSION

# 4 Ausgewählte Anwendungsfälle von pfSense

In diesem Kapitel soll die Implementierung praxisnaher Anwenungsfälle dokumentiert werden um die Möglichkeiten des Systemmanagements von pfSense vorzustellen.

## 4.1 pfSense als DSL-Router im Heimbereich

In diesem ersten Konfigurationsbeispiel erfolgt der Internetzugang über

## 4.2 pfSense als redundanter Firewall-Cluster im Firmenumfeld

Hier beginnt der zweite Unterabschnitt des zweiten Hauptteils.

VORABVERSION

# 5 Schluss

Dies ist der Schlussteil. Abschließende Empfehlung

VORABVERSION

# 6 Glossar

**DHCP-Server** DHCP steht als Abkürzung für "Dynamic Host Configuration Protokoll" und beschreibt Techniken um Hosts in Netzwerken dynamisch Netzwerkparameter wie IP-Adressen zuzuweißen[8]

**Router** Ein Rechnersystem mit mindestens zwei Netzwerkschnittstellen, das Netzwerkschverkehr zwischen diesen Netzwerkschnittstellen nach einem Regelwerk vermittelt und weiterleitet.

**Routerdistribution** Eine spezielle Art von Betriebssystem, deren Hauptaugenmerk bei der Konzeption und Entwicklung darauf liegt Router-Funktionen sicher und stabil auszuführen

**VLAN** Die Abkürzung VLAN steht für Virtual Local Area Network und fasst Techniken zusammen um physikale Netzwerkstrukturen logisch zu Segmentieren, beispielsweise zur Erhöhung der Sicherheit oder um Broadcast-Domänen zu verkleinern.

CARP pf pfsync XMLRPC BSD FreeBSD OpenBSD linux Betriebssystem BSD-Lizenz GPL-Lizenz Cluster(HA,HP, ) Intel, BSD-Jails

VORABVERSION

[8] [10]

# 7 Literatur- und Quellenverzeichnis

## Literaturverzeichnis

[1] Michael W. Lucas: *Absolute BSD (2nd Edition). The Ultimate Guide to FreeBSD*. No Starch Press, 2008,
ISBN: 978-1-59327-151-0

[2] Peter N.M. Hansteen: *The Book of PF*. No Starch Press, 2008,
ISBN: 978-1-59327-165-7

[3] Christopher M. Buechler, Jim Pingle: *pfSense: The Definitive Guide*. Reed Media Services, 2009,
ISBN: 978-0-97903-428-2

## Quellenverzeichnis

[1] http://www.ipcop.org/1.4.0/en/install/html/
Abrufbar am 16.12.2012.

[2] http://www.ipcopwiki.de/index.php/Samba_Server
Abrufbar am 20.12.2012.
*Anmerkung: Der Artikel zu diesem Addon ist zwar noch verfügbar, jedoch nicht die eigentlichen Dateien, die für das Addon erforderlich sind.*

[3] http://www.ipcop.org/2.0.0/en/admin/html/whatsnew.html
Abrufbar am 11.01.2013.

[4] http://wiki.ipfire.org/de/addons/start
Abrufbar am 10.01.2013.

[5] http://www.gnu.org/licenses/gpl.html
Abrufbar am 20.02.2013

[6] http://www.freebsd.org/docs.html
Abrufbar am 21.02.2013

[7] http://www.freebsd.org/copyright/freebsd-license.html
Abrufbar am 20.02.2013

VORABVERSION

[8] http://www.freebsd.org/doc/de/books/faq/hardware.html#which-hardware-to-get
Abrufbar am 12.01.2013.

[9] http://wiki.ipfire.org/de/addons/mdadm/starten
Abrufbar am 16.02.2013.

[10] http://www.isc.org/software/dhcp
Abrufbar am 11.01.2013.

[11] https://www.euro-ix.net/documents/1024-Euro-IX-IXP-Report-pdf
Abrufbar am 18.02.2013

[12] http://www.bsdcan.org/2006/papers/BSD_Firewalling.pdf
Abrufbar am 19.02.2013

VORABVERSION