IPCop-Administrationshandbuch

Übersetzer: Christian Werner-Meier, dotzball, enricoballa, Fast.Edi, Dirk Jelin, zisoft
docbook-Umsetzung: zisoft

IPCop-Administrationshandbuch

von
Übersetzer: Christian Werner-Meier, dotzball, enricoballa, Fast.Edi, Dirk Jelin, zisoft
docbook-Umsetzung: zisoft

Veröffentlicht 2006

Inhaltsverzeichnis

Vorwort

1. Rechte und Haftungsausschlüsse

IPCop ist Copyright-geschützt von der "IPCop Linux Group".

IPCop Linux wird unter der GNU (General Public License) veröffentlicht. Für mehr Informationen besuchen Sie bitte die offizielle IPCop-Webseite [http://www.ipcop.org]. Sie können es in Teilen oder komplett kopieren, solange die Kopien der Copyright-Erklärung entsprechen. Die Informationen die in diesem Dokument enthalten sind können sich zwischen dieser und der nächsten Version ändern.

Alle Programme und Angaben die in diesem Dokument enthalten sind wurden mit bestem Wissen und Gewissen und nach sorgfälltigem Testen erstellt und entwickelt. Trotzdem können Fehler nicht zu 100% ausgeschlossen werden. Daher kann IPCop keine Garantie dafür übernehmen, das Fehler durch dieses Dokument oder Folgeschäden durch Verfügbarkeit, Leistung oder Gebrauch dieser oder verwandter Materialien entstehen.

Der Gebrauch von Namen, im Allgemeinen der Gebrauch von Firmennamen, Handelsnamen, usw. innerhalb diesem Dokument (auch ohne spezieller Darstellungsart) bedeutet nicht, dass diese Namen als#„frei“ im Sinne des Gesetzes bezüglich des Warenzeichens betrachtet werden können und das sie von jedermann benutzt werden dürfen.

Alle Handelsnamen werden ohne Erlaubnis auf freien Gebrauch benutzt. Sie könnten registrierte Warenzeichen sein. Als generelle Richtlinie hält sich IPCop an die Notation der Hersteller. Andere Produkte die hier genannt werden können Warenzeichen des jeweiligen Herstellers sein.

1. Ausgabe - 29. Dezember 2001

Verfasser/in: Charles Williams

Ich danke allen die das Dokument geprüft und korrigiert haben: Harry Goldschmitt, Mark Wormgoor, Eric S. Johansson und der Rest der "IPCop Linux Group".

2. Ausgabe - 10. Januar 2003

Verfasser/in: Chris Clancey, James Brice, Harry Goldschmitt, und Rebecca Ward

3. Ausgabe - 25. April 2003

Verfasser/in: Chris Clancey, Harry Goldschmitt, und Rebecca Ward

4. Ausgabe - 25. September 2004

Verfasser/in: Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander und Peter Walker

2. Allem voran ...

Hallo. Im Namen unseres Projektleiters, Jack Beglinger, möchten Sie die Dokumentationsmitarbeiter mit diesem IPCop Administrationsdokument willkommen heißen. Wir möchten diese Gelegenheit nutzen und uns dafür bedanken das Sie unsere Firewall ausprobieren und hoffen das Sie alle Ihre Bedürfnisse befriedigt. Das Team möchte außerdem der IPCop Linux Community danke für Ihre konsequente Präsenz und der herausragenden Hilfestellungen sowohl für neue als auch für erfahrende Benutzer. Ferner möchten wir dem "SmoothWall Team" dafür danken das sie die IPCop Linux Community zusammen gebracht hat.

Egal ob Sie ein Langzeitbenutzer sind der sich entlang der Versionskette bewegt oder ein neuer Benutzer der sich gerade auf seine erste Installation vorbereitet, wir hoffen, dass Sie all' das in dieser Anleitung finden was Sie brauchen, um loslegen und um langfristig arbeiten zu können. Falls, aus welchen Gründen auch immer, hier irgend etwas nicht abgedeckt und Sie denken es sollte aber, dann kontaktieren Sie uns und lassen es uns wissen. Wir freuen uns immer, von unseren Benutzern zu hören (eigentlich fühlen sich einige von uns sogar ein wenig alleine während sie jeden Tag vor ihren Computern sitzen und daher ist eine kleine Nachricht ab und an eine nette Abwechslung) und hoffen so gut es geht bei ihren Bedürfnissen behilflich zu sein. Nun können Sie sich

entspannen und das Internet geniessen ohne sich Sorgen machen zu müssen.

So, hier sind ein paar Informationen für diejenigen unter Ihnen, die die Zeit haben diese zu lesen und auf die Installation der IPCop-Linux-Box warten. Die Anfangsveröffentlichung von IPCop war ein vorläufiges Release um uns beim Finden von Problemen in der IPCop Linux Distribution zu helfen. Wir sind nun schon beim dritten "full release". Falls es doch passieren sollte das Sie ein Problem finden, dann schauen Sie bitte erst die IPCop FAQ nach. Wir versuchen stehts die FAQ aktuell zu halten sobald wir ein Problem finden. Sie können uns auch mit Informationen zum bearbeiten und lösen von Problemen mitteilen.

Falls Ihr Problem nicht in der FAQ auftaucht, dann können Sie uns auch per IRC erreichen (Server: irc.openprojects.net Channel: #ipcop), die "IPCop mailing list" kontaktieren oder schicken Sie der IPCop Linux Group eine email für direkten Support. Sie sind immer gut beraten wenn Sie eine der ersten drei Methoden nutzen falls sie eine schnelle Antwort und Lösung haben wollen. Die IPCop Linux Group direkt zu kontaktieren kann zu erheblichen Verzögerungen führen, abhängig von Ihrem Erfahrungsgrad.

Sie können weitere Informationen wie auch die neuesten FAQ, mailing list Informationen und die IPCop Linux Group Kontaktinformationen auf unserer Webseite finden: *IPCop Webseite* [http://www.ipcop.org]

Kapitel 1. Einleitung der Projektleiter

Willkommen und Danke für Ihr Interesse an IPCop.

1.1. Was ist IPCop?

Nun, was ist IPCop?

1. IPCop ist eine Firewall; zu aller erst, zu letzt und überhaupt.

2. IPCop ist eine spezialisierte Linux Distribution; komplett, konfiguriert, und fertig um Ihr Netzwerk zu schützen. Ferner, es fällt unter die GNU General Public License [http://www.gnu.org/licenses/gpl.html], d.h. der komplette Quellcode kann heruntergeladen und überprüft werden, oder einfach von Ihnen für Ihre persönlichen Vorlieben oder aus eigenen Sicherheitsgründen modifiziert und/oder rekompiliert werden.

3. IPCop ist eine Community; wo Mitglieder einander helfen und alle sich beteiligen das Projekt und sich gegenseitig zu verbessern. Diese Unterstützung beginnt beim simplen # „Networking 101“#-Typ durch Instruktionen und Anweisungen bis hin zur Hilfestellung für Mitglieder beim Anpassen ihrer IPCop um spezielle Bedürfnisse wie z.B. Net-Phones (VoIP) oder Multiple-Büro-Integrität zu bewältigen.

Das war eine Fangfrage. Die richtige Antwort ist: Alles von dem oben genannten.

Hintergrund:

IPCop entstand durch unterschiedlichste Bedürfnisse. Das erste dieser Bedürfnisse war der Wunsch nach einem sicheren Schutz unserer privaten und gewerblichen Netzwerke. Als IPCop im Oktober 2001 begann, standen schon andere Firewalls zu Verfügung. Trotzdem hatte das Team das IPCop startete das Gefühl, dass die anderen zwei Bedürfnisse die IPCOP erfüllt bisher nicht befriedigt wurden; GPL und ein Gefühl der Community.

Die IPCop-Gründungsgruppe entschloss sich die Dinge anders anzupacken. Sie nahm den "base GPL code" einer vorhandenen Firewall und begann eine neue mit Hinblick darauf, die Bedürfnisse der User-Community in den Vordergrund zu stellen. Wegen dieser Bedürfnisse ist es der Wunsch der Benutzer den IPCop den eigenen zu nennen, Verbesserungen zu installieren, oder einfach dazu zu lernen indem man sich ansieht was andere vollbracht haben. Diese Bedürfnisse sind der Grund weswegen der Aufbau von IPCop so von den Verbesserungen profitiert. Direkt zu hören und zu sehen was getan wurde und warum. Die Community lässt IPCop wachsen und IPCop verhilft der Community zu Wachstum.

Jetzt, nach mittlerweile 2 1/2 Jahren, wurde die erste Grundüberholung von IPCop veröffentlicht. Ihr wurden viele coole Sachen hinzugefügt; vierfache Netzwerkunterstützung, Einbruchsdetektion für alle Netzwerke und ein schickes neues Interface, nur um ein paar zu nennen.

Und nun nochmals; Willkommen zu IPCop!

Jack Beglinger
Projektleiter

1.2. Teilliste der Ausstattung

- IPTable-Netzwerkfilter
- IDE-, SCSI- und CF- (Disk on a Chip) Laufwerkunterstützung.
- 4-fach Netzwerkunterstützung:
  - GRÜN — Internes vertrauenswürdiges Netzwerk
  - BLAU — Wireless teil-vertrauenswürdiges Netzwerk (kann als zweites grün benutzt werden)
  - ORANGE — DMZ für im Internet erreichbare Server
  - RED — Die Internetverbindung per:
    - Einwahlmodem (analog)

    - ISDN
    - Netzwerkverbindung zu:
        - DSL-Modem
        - Kabel-Modem
    - USB-Verbindung zu (passende Treiber vorausgesetzt):
        - DSL-Modem
        - Kabel-Modem
- Mehrere #„Real“-IPs werden auf ROT unterstützt wenn statische IPs verwendet werden.
- DHCP-Client für ROT wird unterstützt um eine IP vom ISP zu empfangen; ebenfalls wird eine Aktualisierung des „dynamic-DNS“ unterstützt, wenn sich die IP ändert.
- DHCP-Server für GRÜN und BLAU um die Netzwerkeinrichtung und -verwaltung zu vereinfachen.
- NTP-Server und Client um die Uhrzeit des IPCop zu setzen und um den internen Netzwerken GRÜN und BLAU eine allgemeine Uhrzeit zur Verfügung zu stellen.
- Einbruchsdetektion für ALLE Netzwerke (ROT, ORANGE, BLAU und GRÜN)
- „Virtuelle Private Netzwerke“ (VPN) erlaubt es mehreren einzelnen Verbindungen sich zu einem gemeinsamen großen Netzwerk zusammen zu schliessen.
- Proxy-Unterstützung erleichtert die Netzwerk-Einrichung und ermöglicht „schnelleres“ Surfen und DNS-Unterstützung.
- Die Administration ist über ein sicheres Webinterface möglich:

    - Grafische Anzeige für CPU, Speicher und Festplatte sowie den Netzwerkdurchsatz

    - Darstellung von Protokollen mit automatischer Sortierung

    - Vielfache Sprachunterstützung.
- Verwendung von älterer Hardware. 386 oder besser. Version 1.4 wurde auf einem 486SX25 mit 12 MB RAM und einer 273 MB Festplatte getestet. Das war das Älteste und Kleinste, was wir zum Zeitpunkt des Tests finden konnten. Es wurde per Netzinstallation installiert und unterstützte die komplette Kabel-Modem-Geschwindigkeit von 3 Mb/s.

1.3. Danksagung

Die IPCop-Software ist zum einen ein gemeinschaftliches Projekt und zum anderen baut es auf einer großen Pionierarbeit auf. Diese Danksagung will einige herausstellen die direkt und indirekt helfen. Sie will jedoch niemals diejenigen unerwähnt lassen, die sich abmühten zu helfen, dass sich das Projekt entwickelt. Ich habe es jedoch nicht geschafft sie alle hier zu nennen. An diese alle: Vielen Dank und entschuldigt, dass ich Euren Namen vergessen habe zu nennen.

An den Rest, dank Euch! Für noch mehr Nennungen schauen Sie bitte unter System#Danksagung im IPCop nach.

Hauptteam

- Mark Wormgoor — leitender Entwickler
- Alan Hourihane — SMP & SCSI Entwickler
- Giles Espinesse —
- Harry Goldschmitt — Leitung Dokumentation
- Eric Oberlander — Entwickler & Übersetzungskoordinator

Entwickler. Mark Wormgoor, Alan Hourihane, Eric S. Johansson, Darren Critchley, Robert Kerr, Gilles Espinasse, Steve Bootes, Graham Smith, Robert Wood, Eric Oberlander, Tim Butterfield and David Kilpatrick.

Dokumentation. Harry Goldschmitt, Chris Clancey, John Kastner, Eric Oberlander, Peter Walker

Übersetzer.

- **Brasilianisches Portugisisch:** Edson-Empresa, Claudio Corrêa Porto, Adilson Oliveira, Mauricio Andrade, Wladimir Nunes
- **Chinesisch:** Vince Chu, Yuan-Chen Cheng, Sohoguard
- **Tschechisch:** Petr Dvoracek, Jakub Moc

- **Dänisch:** Michael Rasmussen
- **Holländisch:** Gerard Zwart, Berdt van der Lingen, Tony Vroon, Mark Wormgoor
- **Finnisch:** Kai Käpölä
- **Französisch:** Bertrand Sarthre, Michel Janssens, Erwann Simon, Patrick Bernaud, Marc Faid'herbe, Eric Legigan, Eric Berthomier, Stéphane Le Bourdon, Stéphane Thirion, Jan M. Dziewulski,spoutnik, Eric Darriak, Eric Boniface
- **Deutsch:** Dirk Loss, Ludwig Steininger, Helmet, Markus, Michael Knappe, Michael Linke, Richard Hartmann, Ufuk Altinkaynak, Gerhard Abrahams, Benjamin Kohberg, Samuel Wiktor
- **Griechisch:** Spyros Tsiolis, A. Papageorgiou, G. Xrysostomou
- **Ungarisch:** Ádám Makovecz, Ferenc Mányi-Szabó
- **Italienisch:** Fabio Gava, Antonio Stano, Marco Spreafico
- **Latein Spanisch:** Fernando Diaz
- **Norwegisch:** Morten Grendal, Alexander Dawson, Mounir S. Chermiti, Runar Skraastad, Alf-Ivar Holm
- **Polnisch:** Jack Korzeniowski, Piotr, Andrzej Zolnierowicz
- **Portugisisch:** Luis Santos, Renato Kenji Kano, Mark Peter, Wladimir Nunes, Daniela Cattarossi
- **Rumänisch:** Viorel Melinte
- **Russisch/Ukrainisch:** Vladimir Grichina, Vitaly Tarasov
- **Spanisch** Curtis Anderson, Diego Lombardia, Mark Peter, QuiQue Soriano, David Cabrera Lozano, Jose Sanchez, Santiago Cassina, Marcelo Zunino, Alfredo Matignon
- **Schwedisch:** Anders Sahlman, Christer Jonson
- **Türkisch:** Ismail Murat Dilek, Emre Sumengen
- **Vietnamesisch:** Le Dinh Long

Andere Projekte und Firmen: Traverse Technologies — Verbesserter Dual ISDN und DOV Support, Linux from Scratch (LFS) — Quellcode für IPCop 1.4, FreeSwan und OpenFreeSwan — IPSec- und VPN-Software, Smoothwall — originale Grundlage und Inspiration, sowie Andere, deren Aufzählung zu umfangreich wäre, um genannt zu werden.

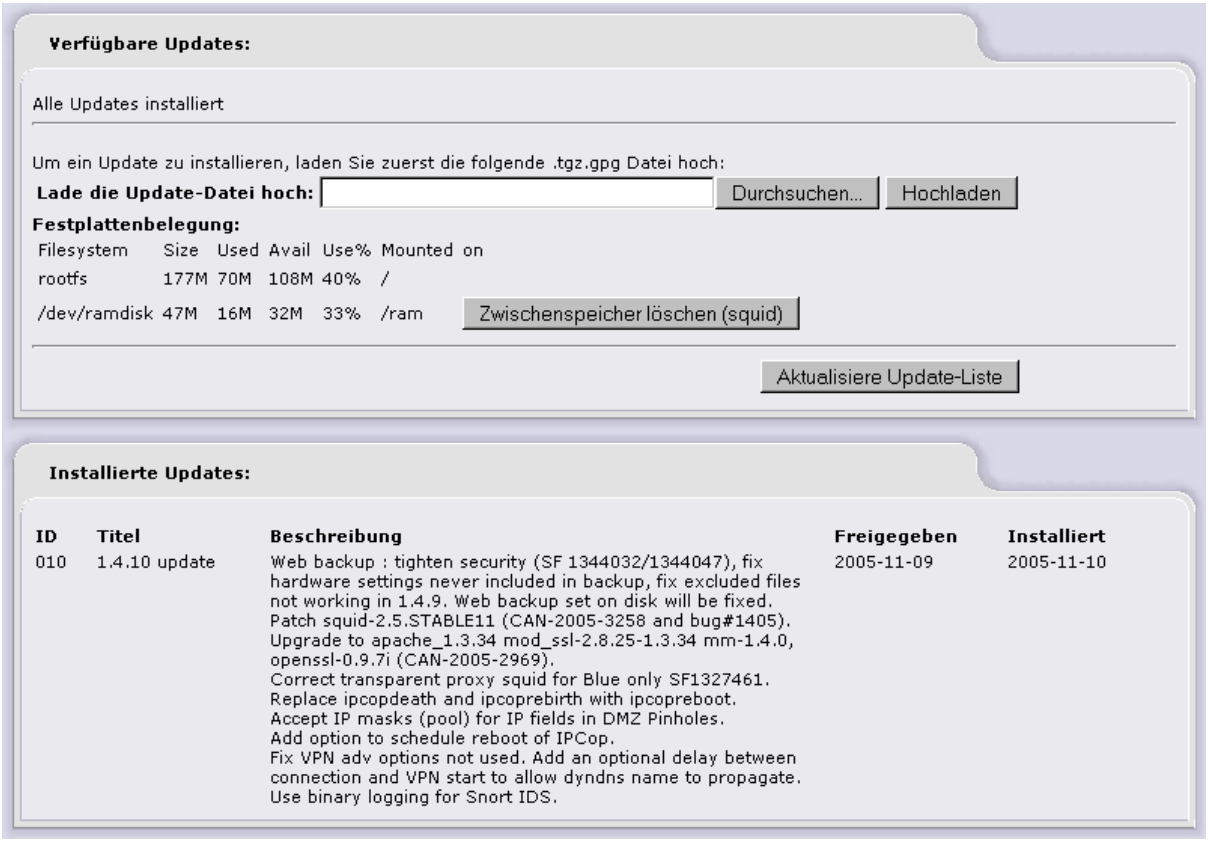
Kapitel 2. Administration und Konfiguration

2.1. System

Diese Seiten dienen dazu, administrative Tätigkeiten am IPCop-Server an sich durchzuführen. Sie erhalten Zugriff auf diese Seiten, indem Sie das Menü System auswählen. Folgende Auswahlen stehen dann im Drop-down-Menü zur Verfügung:

- Startseite — Zurück zur Startseite
- Updates — Überprüfung auf neue Updates und Einspielen von Updates
- Passwörter — Ändern des Passworts für den Benutzer admin und/oder den Benutzer dial
- SSH Zugriff — SSH-Zugriff aktivieren und konfigurieren
- Einstellungen der Benutzeroberläche — JavaScript für die Benutzung des Webinterfaces aktivieren/deaktivieren sowie Festlegung der Sprache des Webinterfaces
- Datensicherung — Erstellt Backups der IPCop-Einstellungen, entweder in Dateien oder auf Diskette. Hierüber können Sie erstellte Backups auch wieder einspielen.
- Herunterfahren — IPCop herunterfahren oder neustarten
- Dank an...— Diese Seite führt alle freiwilligen Helfer auf, die an der Entwicklung von IPCop beteiligt waren

2.1.1. Updates



Dieser Bereich hat 3 Abschnitte:

1. Den aktuellen Stand
2. Informationen über die Verfügbarkeit neuer Updates
3. Einspielen von Updates

Jedesmal, wenn IPCop eine Verbindung ins Internet aufbaut, wird überprüft, ob neue Updates verfügbar sind. Sie können auch manuell auf Updates prüfen, indem Sie den Schalter Akutalisiere Update-Liste klicken. Wenn ein neues Update verfügbar ist, wird dies angezeigt zusammen mit einer kurzen Beschreibung und einem Link „Info“. Wenn Sie dem Link folgen, gelangen Sie zu einer Seite mit allen relevanten Informationen über das Update sowie einem Download-Link.

Wenn Sie das Update herunterladen, wird die Datei auf der Maschine gespeichert, auf der Ihr Web-Browser läuft, nicht auf dem IPCop. Benutzen Sie den Schalter Durchsuchen, geben Sie die heruntergeladene Update-Datei an und klicken Sie auf Hochladen, um das Update zu installieren.

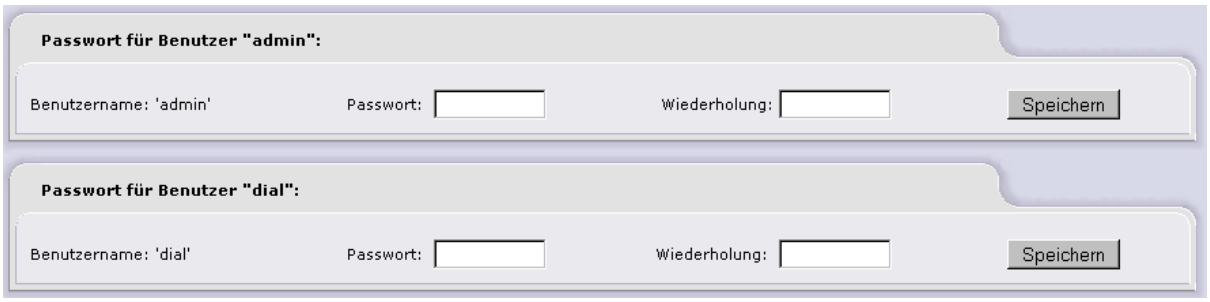
Anmerkung

Der Opera Browser verarbeitet Updates nicht korrekt und sollte deshalb nicht verwendet werden, um Updates auf dem IPCop einzuspielen.

Anmerkung

Nur offizielle IPCop-Updates werden auf dem IPCop installiert. Einige Updates führen einen automatischen Neustart des IPCops aus, lesen Sie deshalb bitte **alle** Update-Informationen, bevor Sie ein Update installieren.

2.1.2. Passwörter

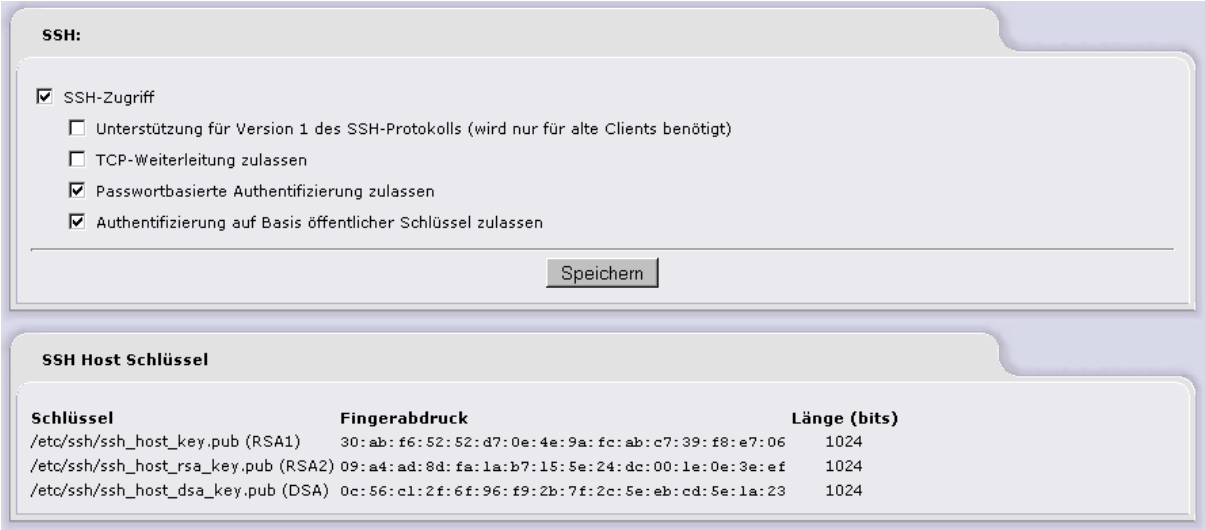


Die Seite Passwörter ermöglicht es, die Passwörter der Benutzer admin und/oder dial zu ändern. Geben Sie einfach das gewünschte Passwort mit Wiederholung in die vorgesehenen Eingabefelder ein und klicken Sie auf Speichern.

Die Eingabe eines Passworts für den Benutzer dial aktiviert diesen Benutzer. Dieser spezielle Benutzer kann die Verbindungsschalter auf der Startseite betätigen, hat aber keinen Zugriff auf die anderen administrativen Seiten des Webinterfaces. Verwenden Sie diesen Benutzer, wenn Sie eine Einwahlverbindung konfiguriert haben und Anwendern erlauben wollen, die Verbindung zum Internet herzustellen, ohne dass diese auch administrativen Zugang zum IPCop erhalten sollen.

2.1.3. SSH-Zugriff

Über die Seite SSH-Zugriff können Sie festlegen, ob SSH-Fernzugriff für Ihren IPCop möglich sein soll, oder nicht. Mit einem gesetzen Häkchen wird der SSH-Fernzugriff aktiviert, ausserdem können Sie hier noch verschiedene Parameter für den SSH-Daemon-Prozess konfigurieren. Der SSH-Zugriff ist in der Standardkonfiguration deaktiviert und sollte **nur wenn nötig aktiviert und anschließend wieder deaktiviert werden**.



So wie die HTTP und HTTPS Ports des IPCop auf 81 und 445 geändert wurden, ist auch der SSH Port auf 222 geändert. Wenn Sie eine GUI-basierte Applikation benutzen, um auf Ihre IPCop-Maschine zuzugreifen, denken Sie daran, den Port 222 anzugeben. Wenn Sie ssh, scp oder sftp Kommandos benutzen, beachten Sie, dass die Syntax zur Angabe des Ports von Kommando zu Kommando verschieden ist. Angenommen, die IP-Adresse Ihres IPCops lautet 192.168.254.1, dann lauten diese Kommandos:

SSH

```
$ ssh -p 222 root@192.168.254.1
```

SCP

```
$ scp -P 222 some/file root@192.168.254.1:
```

SFTP

```
$ sftp -o port=222 root@192.168.254.1
```

Benutzen Sie ggf. die Dokumentation (man pages) dieser Kommandos für weitere Beispiele.

2.1.3.1. SSH-Optionen

Folgende SSH-Optionen können über die Seite konfiguriert werden:

SSH-Zugriff:	Ein gesetztes Häkchen aktiviert den SSH-Zugriff. Wenn der externe Zugang nicht aktiviert ist, ist SSH nur über das GRÜNE Netz erreichbar. Mit aktiviertem SSH-Zugriff kann sich jeder, der das IPCop root Passwort kennt, auf der IPCop Kommandozeile einloggen.
Unterstützung für Version 1 des SSH-Protokolls (wird nur für alte Clients benötigt)	Diese Box aktiviert die Unterstützung des SSH Version 1 Protokolls. Von der Verwendung dieser Option wird dringend abgeraten, da bekannte Sicherheitslücken der Version 1 existieren. Benutzen Sie diese Option nur für kurzfristigen Zugang, wenn Sie nur SSH-Klienten verfügbar haben, die nur Version 1 unterstützen und die nicht auf Version 2 aktualisert werden können. Die meisten aktuellen SSH-Klienten unterstützen Version 2.

zulassen — Diese Option ermöglicht SSH-verschlüsselte Tunnelverbindungen aufzubauen.

Wozu dient sowas, wenn IPCop bereits ein VPN besitzt?

Sie sind unterwegs und auf einem Ihrer Server tritt ein Problem auf. Sie bekommen keine VPN Roadwarrior Verbindung. Wenn Sie das root-Passwort des IPCops kennen, können Sie SSH Portweiterleitung verwenden, um durch Ihre Firewall Zugang zu Ihrem Server im geschützten Netzwerk zu erhalten. Die nächsten Abschnitte zeigen, wie man so etwas aufsetzt. Dabei wird angenommen, dass ein Telnet-Server auf einem internen Rechner mit der IP-Adresse 10.0.0.20 läuft. Ausserdem wird angenommen, dass die Remote-Maschine ein Linux-Rechner ist. Putty für Windows hat die gleichen Fähigkeiten, diese werden aber über Dialogboxen erreicht.

1. Richten Sie externen Zugang für den HTTPS Port 445 ein.
2. Konfigurieren Sie den SSH-Zugriff, die Portweiterleitung und den externen Zugang für den Port 222 über das IPCop Webinterface.
3. Bauen Sie einen SSH-Tunnel zwischen der Remote-Maschine und dem internen Server (auf dem ein SSH-Daemon läuft) mit folgendem Kommando auf:

```
$ ssh -p 222 -N -f -L 12345:10.0.0.20:23 root@ipc
```

-p 222	IPCop überwacht SSH auf Port 222, nicht auf dem Standard-Port 22.
-N	Lässt SSH in Verbindung mit -f im Hintergrund laufen, ohne die Verbindung zu beenden. Wenn Sie diese Option verwenden, müssen Sie kill benutzen, um den SSH-Prozess zu beenden. Alternativ können Sie den Befehl **`sleep 100`** An das Ende der Kommandozeile anhängen und die -N Option weglassen. In diesem Fall wird der SSH-Prozess nach 100 Sekunden beendet, aber die telnet-Sitzung und der aufgebaute Tunnel bleiben bestehen.
-f	SSH läuft im Hintergrund.
-L	Weist SSH an, einen Port-Weiterleitungs-Tunnel aufzubauen, der mit den nächsten Parametern spezifiziert wird.
12345	Der lokale Port, der für den Tunnel zum Remote-Service verwendet wird. Sollte größer als 1024 sein, andernfalls müssen Sie als root angemeldet sein, um Standard-Ports benutzen zu können.
10.0.0.20	GRÜNE Adresse des Remote-Servers.
23	Zu benutzender Remote-Port, Telnet.
root@ipcop.fqn	Legt fest, dass die IPCop Firewall als Port-Weiterleitungs-Agent benutzt wird. Sie benötigen eine Benutzer-ID für die Anmeldung und die einzige verfügbare ist root. Sie werden aufgefordert, das root-Passwort für den IPCop einzugeben.

4. Abschließend loggen Sie sich beim Remote-Telnet mittels des Tunnels ein.

```
$ telnet localhost 12345
```

localhost ist die lokale Maschine, auf der Sie sich befinden. Die loopback-Adresse 127.0.0.1 ist als localhost definiert. 12345 ist der lokale Tunnelport, der im vorherigen Kommando festgelegt wurde.

Ein Tutorial über SSH Port-Weiterleitung finden Sie auf Dev Shed [http://www.devshed.com/c/a/Administration/Secure-Tunnelling-with-SSH/].

Passwortbasierte Authentifizierung zulassen	Ermöglicht es Benutzern, sich beim IPCop mittels des root-Passworts anzumelden. Wenn Sie diese Option ausschalten, müssen Sie zunächst Ihre SSH Schlüsseldateien konfigurieren und sicherstellen, dass Sie sich mit den Schlüsseldateien einloggen können.
Authentifizierung auf Basis öffentlicher Schlüssel zulassen	Mit dieser Option wird die Authentifizierung auf Basis öffentlicher Schlüssel zugelassen. Dies ist die bevorzugte Methode, den SSH-Zugriff auf dem IPCop abzusichern. In diesem Artikel [http://security.itworld.com/4360/LWD010410SSHtips/page_1.html] finden Sie eine Diskussion über die Benutzung von **SSH-keygen**, um RSA-Schlüssel für die Verwendung mit SSH zu erzeugen.

2.1.3.2. SSH Host Schlüssel

Dieser Abschnitt listet die Fingerabdrücke der von IPCop verwendeten SSH-Schlüssel, die Sie verwenden können, um eine SSH-Verbindung mit IPCop zu verifizieren. Wenn Sie das erste Mal eine SSH-Verbindung zum IPCop erstellen, wird der Fingerabdruck angezeigt, und Sie werden aufgefordert, die Korrektheit zu bestätigen. Sie können den angezeigten Schlüssel mit der Darstellung auf dieser Seite vergleichen.

2.1.4. Einstellungen der Benutzeroberfläche

Diese Seite regelt, wie die Seiten des IPCop-Webinterfaces arbeiten und dargestellt werden.

Denken Sie daran, nach jeder Änderung den Speichern Schalter zu betätigen.

Um die Voreinstellungen wiederherzustellen, klicken Sie auf den Schalter Voreinstellungen wiederherstellen.

2.1.4.1. Anzeige

Javascript aktivieren:	Seit Version 1.4.0 verwenden die Seiten JavaScript, um den Bedienungskomfort zu verbessern. Allerdings arbeiten einige Browser nicht korrekt mit JavaScript. Wenn JavaScript abgeschaltet ist, werden keine Drop-Down-Menüs mehr dargestellt und Sie erreichen die einzelnen Auswahl-

	möglichkeiten über Links im oberen Seitenbereich.
Hostname im Fenstertitel anzeigen:	Mit dieser Option aktivieren Sie die Anzeige des Hostnamens oben auf jeder Seite. Dies kann hilfreich sein, wenn Sie mehr als einen IPCop administrieren.
Aktualisere index.cgi Seite während der Verbindung	Standardmässig wird die Startseite aktualisiert, wenn IPCop eine Verbindung ins Internet aufgebaut hat. Ein manueller Klick auf den „Aktualisieren“-Schalter aktualisiert die Seite. Wenn diese Option aktiviert ist, aktualisiert sich die Startseite alle 30 Sekunden automatisch.
Wählen Sie eine Sprache, in der IPCop angezeigt werden soll:	Über dieses DropDown-Menü können Sie eine der zahlreichen Sprachen wählen, mit der die Seiten des Webinterfaces dargestellt werden. Das IPCop-Übersetzerteam plant die Unterstützung weiterer Sprachen, solange freiwillige Helfer bei der Übersetzung helfen. Wenn weitere Übersetzungen verfügbar sind, werden Sie den System-Updates hinzugefügt. Selbstverständlich können Sie die IPCop-Texte selbst in eine andere Sprache übersetzen. Wenn Sie dies tun wollen, setzen Sie sich bitte zuerst mit dem IPCop Übersetzungs-Koordinator, Eric Oberlander, <eoberlander@users.sourceforge.net>, in Verbindung. Er hat den Überblick über alle laufenden Übersetzungsaktivitäten. Für weitere Informationen besuchen Sie bitte die Seite IPCop How To Translate [http://www.ipcop.org/modules.php?op=modload&name=phpWiki&file=index&pagename=HowToTranslate].

2.1.4.2. Klang

Piepen, wenn IPCop verbindet oder trennt	Standardmässig piept IPCop einmal, wenn die Verbindung hergestellt wurde und zweimal, wenn die Verbindung getrennt wird. Deaktivieren Sie diese Option, wenn Sie keine akustischen Signale wünschen. Dies beeinflusst nicht die akustischen Signale beim Starten und Herunterfahren.

2.1.5. Datensicherung

Es gibt zwei Möglichkeiten für die Datensicherung, eine erstellt Dateien, die andere schreibt auf Diskette.

Eine Backup-Diskette begrenzt die zu sichernde Datenmenge auf 1.44 MB. Allerdings ist dies die Methode, mit der bereits während der Installation eine zuvor gesicherte Konfiguration eingespielt werden kann. Sie werden dabei aufgefordert, eine Backup-Diskette einzulegen. Die Daten werden eingespielt und die Installation vervollständigt.

Bei der Datensicherung erstellt IPCop zwei Dateien, eine tar.gz und eine .dat Datei. Ausserdem wird ein eindeutiger Backup-Schlüssel erzeugt, mit dem die tar.gz Datei verschlüsselt wird. Die Bezeichnungen Verschlüsselt und Nichtverschlüsselt sind irreführende Bezeichnungen auf der Datensicherungsseite im Webinterface. Während der Verschlüsselung der .dat Datei wird die Verschlüsselung benutzt, um die .dat Datei zu „signieren“, damit sie nicht versehentlich auf einer anderen IPCop-Maschine eingespielt werden kann. Sobald ein Schlüssel erzeugt wurde, können nur .dat Dateien für eine Wiederherstellung verwendet werden.

Für einen vollständigen Schutz durch eine Datensicherung sollten **alle** in den folgenden Szenarien beschriebenen Methoden und Dateien verwendet werden.

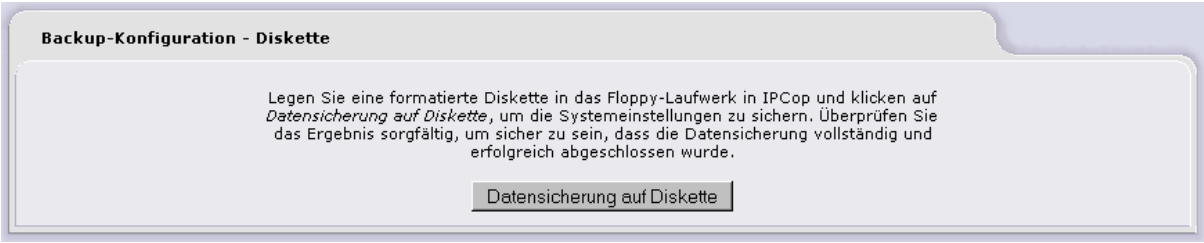
Beschädigte IPCop-Einstellungen	Benutzen Sie die dazugehörige .dat Datei, um die gesicherten Einstellungen wieder herzustellen.
Sie müssen IPCop neu installieren	Benutzen Sie während der Installation eine Backup-Diskette, um zuvor gesicherte Einstellungen einzuspielen. Anschließend importieren Sie die .tar.gz Datei, um die restlichen Einstellungen und Log-Dateien wiederherzustellen.

2.1.5.1. Datensicherung in Dateien

In diesem Bereich der Datensicherungsseite verwalten Sie die Erstellung, Export, Import und Wiederherstellung der IPCop Datei-Backups. Mit dem Schalter Erzeuge erstellt IPCop einen Backup Schlüssel, wenn noch keiner existiert, und erstellt zwei Backup Dateien. Wenn Sie zum ersten Mal Backup Dateien erstellen, ändert sich der Text im Schalter Import .tar.gz in Import .dat. Dadurch wird kenntlich gemacht, dass zukünftig nur noch .dat Dateien importiert werden können. Exportieren Sie beide Dateien auf den PC, auf dem Ihr Webbrowser läuft, indem Sie auf die Export Links klicken.

Wenn Sie von einer Diskette zurückspielen wollen, markieren Sie einen der Datensicherungssätze und klicken Sie auf den Schalter Wiederherstellen. Alternativ können Sie eine .dat Datei von einem anderen PC wiederherstellen.

2.1.5.2. Datensicherung auf Diskette



Mit diesem Bereich der Datensicherungsseite können Sie Ihre IPCop Konfiguration auf einer Diskette sichern. Der einfachste Weg, eine gesicherte Konfiguration wiederherzustellen, ist eine Neuinstallation von CD-ROM oder HTTP/FTP. In einer frühen Phase des Installationsvorgangs werden Sie gefragt, ob Sie eine Diskette mit einer gesicherten Konfiguration einspielen wollen. Wenn das der Fall ist, legen Sie die Diskette in das Laufwerk und wählen Sie Wiederherstellen. Die gesicherte Konfiguration wird dann wiederhergestellt und die Installation abgeschlossen.

Nachdem die Installation abgeschlossen ist, können Sie über das Webinterface eine unverschlüsselte .tar.gz Datei einspielen und damit gesicherte Log-Dateien usw. wiederherstellen.

Warnung

IPCop kann z.Zt. keine DOS-formatierten Disketten beschreiben. Um eine Diskette für IPCop-Backups

zu benutzen, müssen Sie sie für Linux formatieren. Dies geschieht mittels

```
# fdformat /dev/fd0
```

Wenn Sie noch einen anderen Linux-PC besitzten, können Sie die Diskette dort formatieren, andernfalls loggen Sie sich mit SSH oder Putty als root auf dem IPCop ein und führen Sie das Kommando dort aus. **fdformat** fordert nicht zum Einlegen einer Diskette auf, wie das unter DOS der Fall ist. Sie müssen die Diskette vorher in das Laufwerk einlegen.

2.1.5.3. Backup-Konfiguration - Diskette

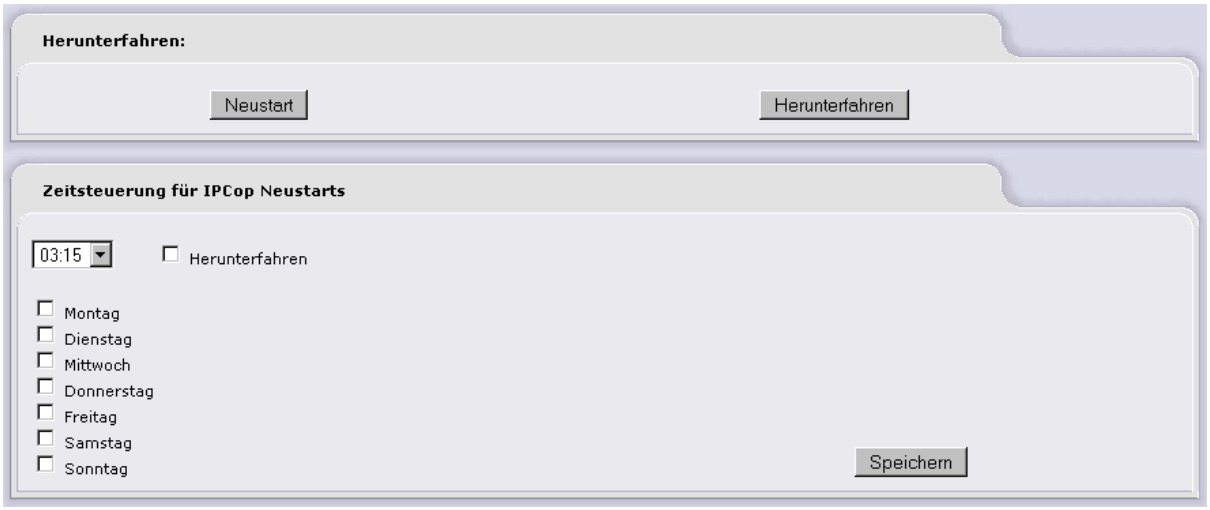
Legen Sie eine Diskette in das Diskettenlaufwerk und klicken Sie den Schalter Datensicherung auf Diskette. Die Konfiguration wird auf Diskette geschrieben und anschließend verifizert.

2.1.5.4. Information

Alle Meldungen, die während einer Datensicherung aufgetreten sind, werden in diesem Bereich dargestellt.

2.1.6. Herunterfahren

Über diese Seite können Sie Ihren IPCop entweder Herunterfahren oder Neustarten. Sie können einfach einen der entsprechenden Schalter klicken, um die Aktion sofort auszuführen, oder die Aktion zu einer bestimmten Zeit einplanen.



2.1.6.1. Herunterfahren

Drücken Sie einen der Schalter Neustart oder Herunterfahren, um die Aktion *sofort* auszuführen.

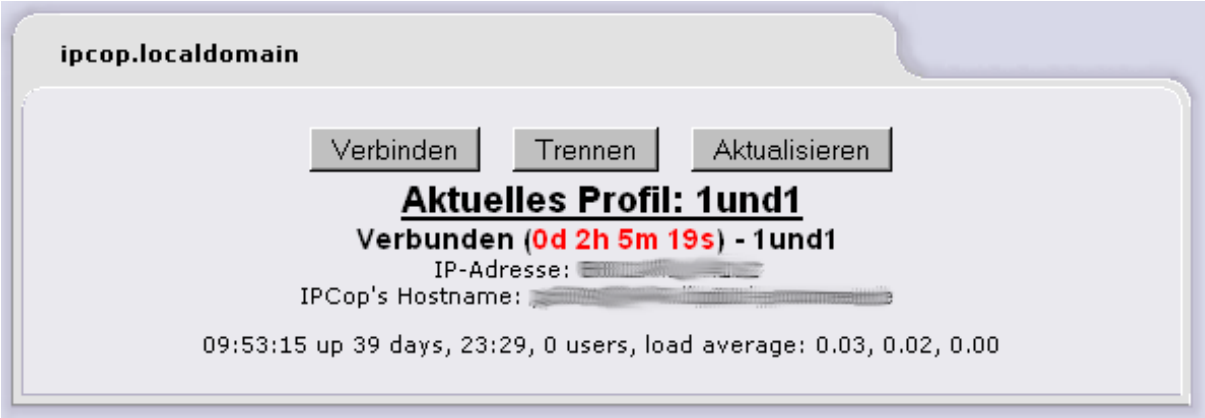
2.1.6.2. Zeitsteuerung für IPCop Neustarts

Seit Version 1.4.10 können Neustarts zeitlich geplant werden. Dazu wird ein cronjob an die **fcrontab** Tabelle angehängt. Um IPCop täglich zu einer bestimmten Zeit neu zu starten, wählen Sie die Zeit aus dem Dropdown-Menü, markieren Sie den oder die Tage und klicken Sie auf Speichern.

Wenn IPCop anstelle eines Neustarts heruntergefahren werden soll, markieren Sie die Box Herunterfahren.

Um eine geplante Aktion zu löschen, entfernen Sie alle Markierungshäkchen und klicken Sie auf Speichern.

2.2. Startseite



Das IPCop-Webinterface erreichen Sie, indem Sie Ihren Webbrowser starten und in die Adresszeile die IP-Adresse der grünen Schnittstelle oder den IPCop-Hostnamen eintragen, gefolgt von der Portangabe 445: https://ipcop:445 oder https://192.168.10.1:445

HTTP-Port 81 wird nicht länger unterstützt

Seit IPCop-Version 1.4.0 werden http-Verbindungen auf Port 81 auf https Port 445 umgeleitet. Als IPCop vor einigen Jahren entwickelt wurde, gab es einige wenige Browser, die nicht mit dem https-Protokoll umgehen konnten, deshalb war das Webinterface auch über http Port 81 erreichbar. Die meisten dieser Browser werden heute nicht mehr benutzt. Da bei http das Passwort im Klartext übermittelt wird, war es eine große Sicherheitslücke, das IPCop-Webinterface über http aufzurufen.

Ändern des HTTPS Ports

Einige Anwender müssen den https Port ändern, da dieser Port von Windows für Verzeichnisdienste verwendet wird (SMB über TCP/IP). Einige Internet-Anbieter haben aus Sicherheitsgründen den Port 445 gesperrt.

Mit dem Kommandozeilentool **setreservedports**, das seit Version 1.4.8 zur Verfügung steht, können die Ports geändert werden.

```
$ /usr/local/bin/setreservedports 5445
```

Hier wird 5445 als Alternativport vorgeschlagen, Sie können aber jeden Port zwischen 445 und 65535 verwenden. Wenn Sie vergessen haben, welche Portnummer Sie verwendet haben, benutzen Sie http und Port 81, um automatisch umgeleitet zu werden.

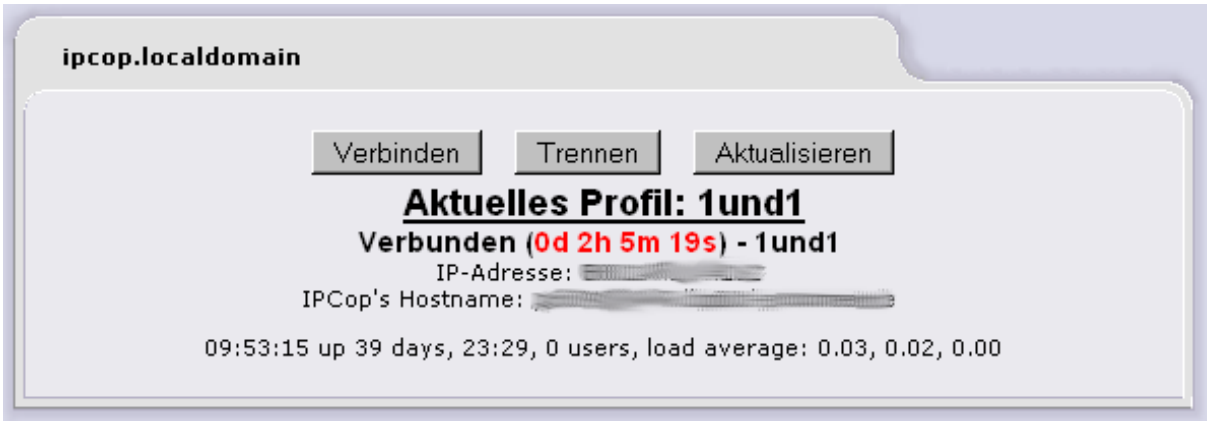
Sie sollten jetzt die Startseite des IPCop-Adminstrations-Webinterfaces sehen. Schauen Sie sich die verschiedenen Optionen und verfügbaren Informationen an. Im Folgenden finden Sie die hauptsächlichen Konfigurations- und Administrationsoptionen, die über das Webinterface erreichbar sind. Wenn Sie sich mit dem System vertraut gemacht haben, fahren Sie mit dem nächsten Abschnitt fort.

Die einzelnen Administrationsseiten des Webinterfaces erreichen Sie über die Menüpunkte im oberen Bildschirmbereich.

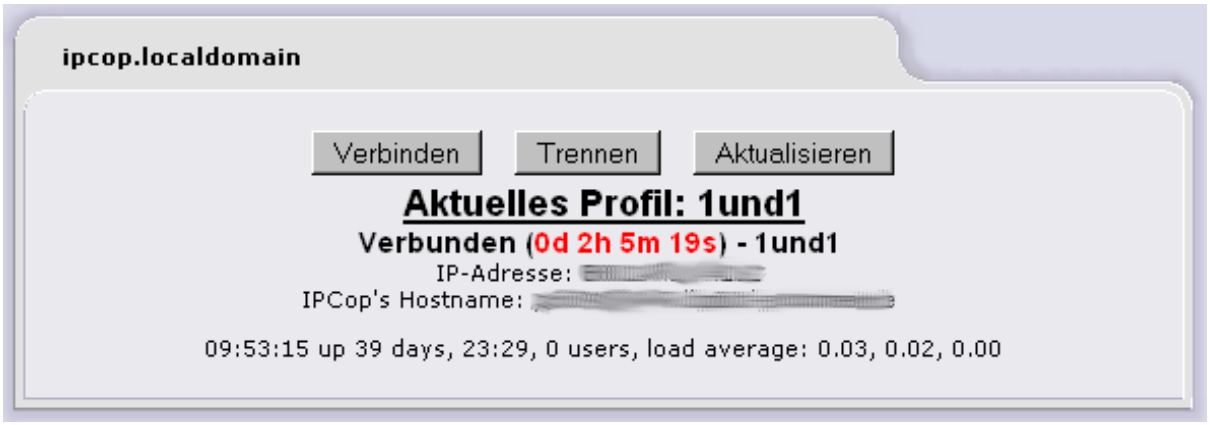
- System Systemkonfiguration und Hilfsfunktionen zum IPCop
- Status Detaillierte Informationen über den Status verschiedener Systembereiche
- Netzwerk Konfiguration/Administration der Einwahl-/PPP-Einstellungen
- Dienste Konfiguration/Administration verschiedener Dienste-Optionen

- Firewall Konfiguration/Administration der Firewall-Einstellungen
- VPN Konfiguration/Administration der VPN (Virtual Private Network)-Einstellungen und Optionen
- Logs Ansicht der Log-Einträge (Firewall, IDS usw.)

Die Startseite ist eine von verschiedenen Seiten, deren Aufbau davon abhängt, wie Sie Ihren IPCop konfiguriert haben.



Wenn alle Einstellungen der PPP-Verbindung korrekt sind und PPP der zu verwendende Verbindungstyp ist, sehen Sie 3 Schalter auf der Hauptseite.



Anmerkung

Sie werden keine aktive Verbindung sehen, bis die Konfiguration abgeschlossen ist.

Oben links sehen Sie den vollständigen Namen Ihrer IPCop-Maschine

Verbindungsschalter

- Verbinden - Stellt die Verbindung mit dem Internet her.
- Trennen - Trennt die aktuelle Verbindung.
- Aktualisieren - Aktualisiert die Startseite.

Zusätzlich zu diesen Schaltern sehen Sie das „Aktuelle Profil“, das für die Verbindung verwendet wird (siehe Einwahl-Seite). Unter dem „aktuellen Profil“ sehen Sie den aktuellen Verbindungsstatus. Dieser kann wie folgt sein:

- Leerlauf - Keine Verbindung und keine Verbindungsversuche.
- Verbinden - Verbindungsversuch läuft.
- Verbunden - Verbunden mit dem Internet.
- Dial on Demand wartet - Momentan nicht verbunden. Wartet auf Aktivitäten eines Clients im Netzwerk, die eine Verbindung erfordern.

Wenn Sie aktuelle mit dem Internet verbunden sind, sehen Sie eine Statuszeile im folgenden Format:

- Verbunden (#d #h #m #s)
- d=Tage verbunden
- h=Stunden verbunden
- m=Minuten verbunden
- s=Sekunden verbunden

Unterhalb der Statuszeile sehen Sie eine Zeile mit folgendem Aufbau:

```
7:07pm up 1 day, 7:21, 0 users, load average: 0.03, 0.01, 0.00
```

Diese Zeile ist die Ausgabe des Linux-Kommandos **uptime** und stellt die aktuelle Uhrzeit, die Anzahl Tage/ Stunden/Minuten, die IPCop seit dem letzten Neustart läuft, die Anzahl der angemeldeten Benutzer und die durchschnittliche Systemlast dar. Zusätzlich sehen Sie, ob Updates verfügbar sind, die noch nicht installiert wurden.

IPCop hat zusätzlich zum root-Benutzer zwei Web-Benutzer. Zum Einen den Benutzer „admin“, mit dem Sie sich am Webinterface anmelden müssen, um Zugang zu den administrativen Seiten zu erhalten. Zum Anderen den Benutzer „dial“. Dieser Benutzer darf nur die Schalter Verbinden oder Trennen auf der Startseite benutzen. Der Benutzer „dial“ ist als Voreinstellung daktiviert, um ihn zu aktivieren, müssen Sie für diesen Benutzer ein Passwort setzen. Auf die Start- und die Danksagungsseite gelangen Sie ohne Passwort, alle anderen Seiten verlangen das „admin“-Passwort.

2.3. Status

Über diese Seiten erhalten Sie Informationen und Statistiken über den IPCop Server. Um zu diesen Seiten zu gelangen, wählen Sie Status aus dem Menü. Folgende Auswahlen stehen in dem Dropdown-Menü zur Verfügung:

- Systemstatus
- Netzwerkstatus
- System-Diagramme
- Netzwerk-Diagramme
- Proxy-Diagramme
- Verbindungen

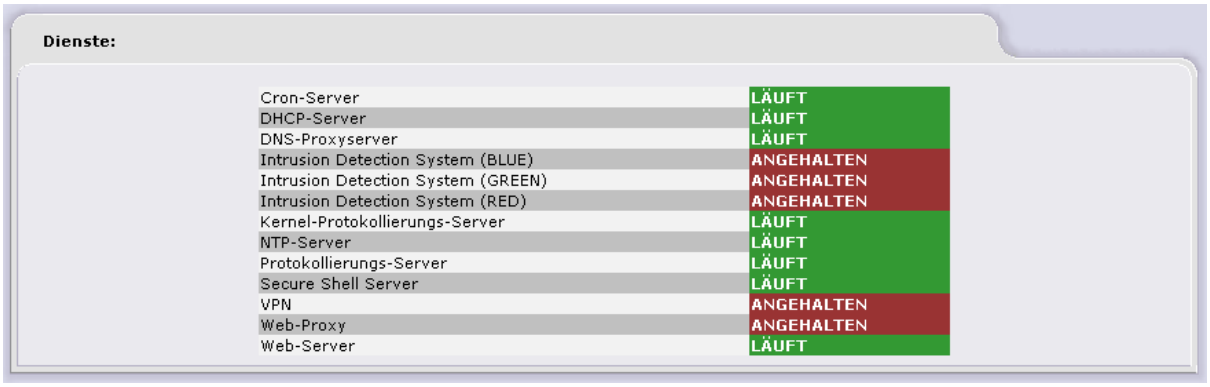
2.3.1. Systemstatus

Die Statusseiten geben eine SEHR genaue Information über den aktuellen Status Ihres IPCop-Servers. Der erste

Abschnitt Systemstatus zeigt die folgenden Informationen:

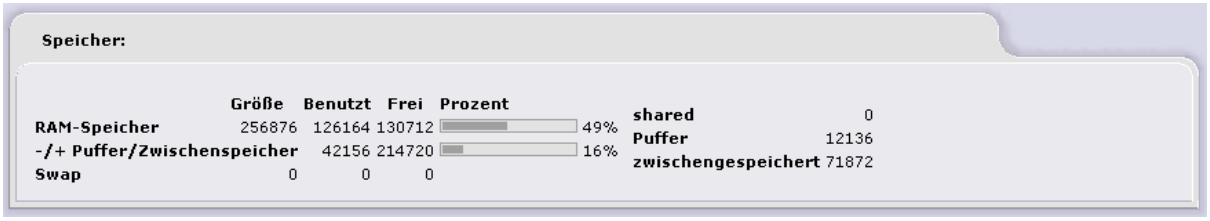
2.3.1.1. Dienste

Dienste - Zeigt, welche Dienste aktuell laufen.



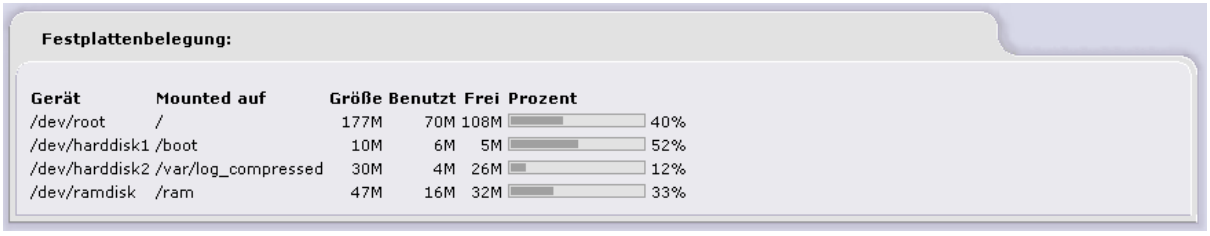
2.3.1.2. Speicher

Speicher - Zeigt die Auslastung von Systemspeicher und Swapfile.



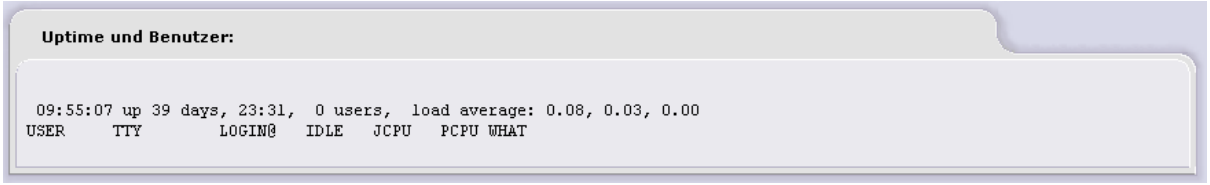
2.3.1.3. Festplattenbelegung

Festplattenbelegung - Zeigt den verfügbaren und belegten Festplattenplatz.



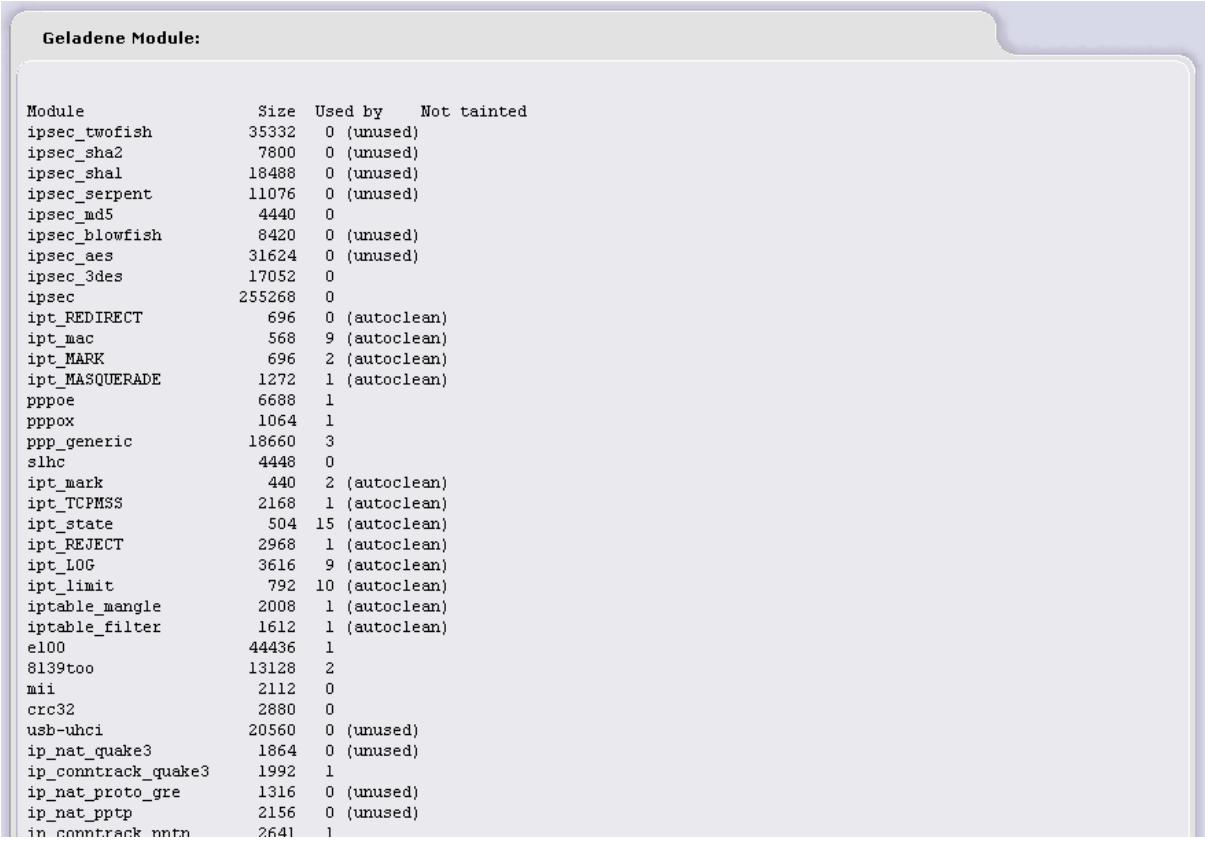
2.3.1.4. Uptime und Benutzer

Uptime und Benutzer - Zeigt die Ausgabe des **uptime** - Kommandos und Informationen über aktuell angemeldete Benutzer.



2.3.1.5. Geladene Module

Geladene Module - Anzeige aller aktuell geladenen und vom Kernel benutzten Module.



Geladene Module:

```
Module                  Size  Used by    Not tainted
ipsec_twofish          35332   0 (unused)
ipsec_sha2              7800   0 (unused)
ipsec_sha1             18488   0 (unused)
ipsec_serpent          11076   0 (unused)
ipsec_md5               4440   0
ipsec_blowfish          8420   0 (unused)
ipsec_aes              31624   0 (unused)
ipsec_3des             17052   0
ipsec                 255268   0
ipt_REDIRECT             696   0 (autoclean)
ipt_mac                  568   9 (autoclean)
ipt_MARK                 696   2 (autoclean)
ipt_MASQUERADE          1272   1 (autoclean)
pppoe                   6688   1
pppox                   1064   1
ppp_generic            18660   3
slhc                    4448   0
ipt_mark                 440   2 (autoclean)
ipt_TCPMSS              2168   1 (autoclean)
ipt_state                504  15 (autoclean)
ipt_REJECT              2968   1 (autoclean)
ipt_LOG                 3616   9 (autoclean)
ipt_limit                792  10 (autoclean)
iptable_mangle          2008   1 (autoclean)
iptable_filter          1612   1 (autoclean)
e100                   44436   1
8139too                13128   2
mii                     2112   0
crc32                   2880   0
usb-uhci               20560   0 (unused)
ip_nat_quake3           1864   0 (unused)
ip_conntrack_quake3     1992   1
ip_nat_proto_gre        1316   0 (unused)
ip_nat_pptp             2156   0 (unused)
ip_conntrack_pptp       2641   1
```

2.3.1.6. Kernel Version

Kernel Version - Informationen über den IPCop-Kernel.

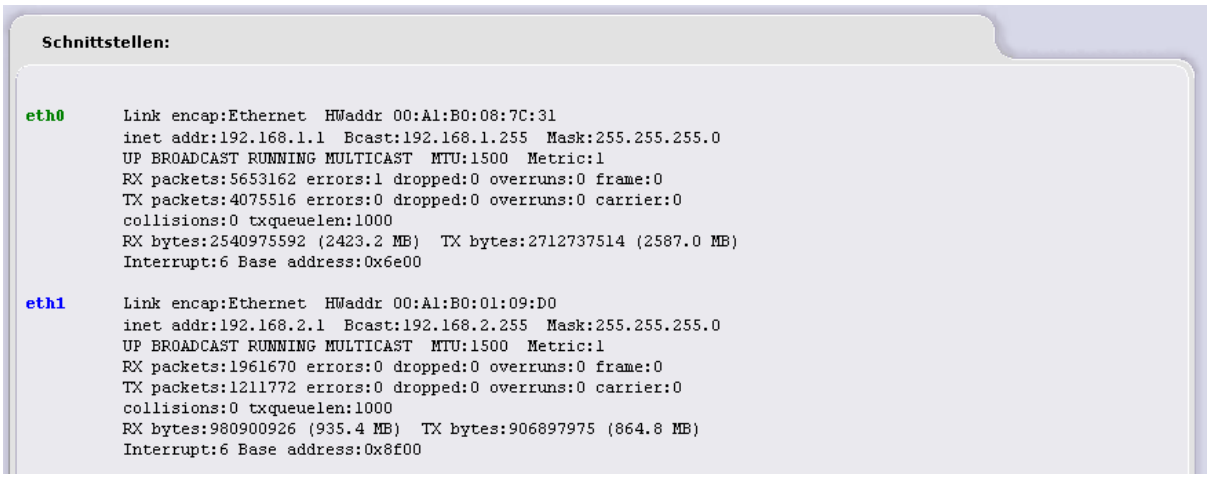
Kernel-Version:

```
Linux ipcop.localdomain 2.4.31 #1 Mon Oct 3 03:37:39 GMT 2005 i586 GenuineIntel unknown GNU/Linux
```

2.3.2. Netzwerk-Status

2.3.2.1. Schnittstellen

Schnittstellen - Dieser Abschnitt gibt Informationen über *alle* Netzwerk-Schnittstellen inkl. PPP, IPSec, Loopback usw.



Schnittstellen:

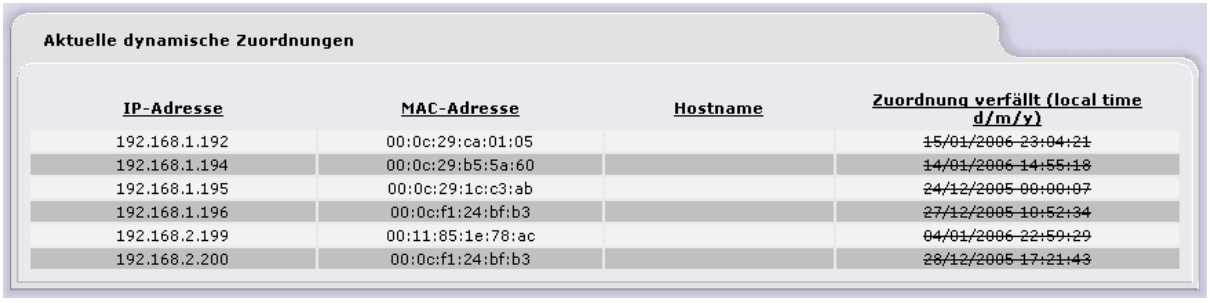
```
eth0      Link encap:Ethernet  HWaddr 00:A1:B0:08:7C:31
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5653162 errors:1 dropped:0 overruns:0 frame:0
          TX packets:4075516 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2540975592 (2423.2 MB)  TX bytes:2712737514 (2587.0 MB)
          Interrupt:6 Base address:0x6e00

eth1      Link encap:Ethernet  HWaddr 00:A1:B0:01:09:D0
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1961670 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1211772 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:980900926 (935.4 MB)  TX bytes:906897975 (864.8 MB)
          Interrupt:6 Base address:0x8f00
```

2.3.2.2. Aktuelle dynamische Zuordnungen

Zeigt die Inhalte der Datei `/var/state/dhcp/dhcpd.leases` wenn DHCP aktiviert ist. Die aktuellen dynamischen Zuordnungen werden aufgeführt, falls verfügbar mit Hostname, sowie der Zeit, zu der die Zuordnung verfällt.

Verfallene Zuordnungen werden durchgestrichen dargestellt.



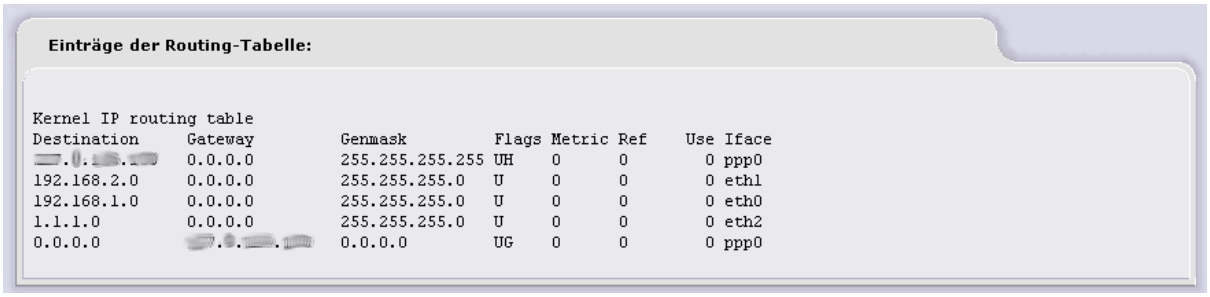
Aktuelle dynamische Zuordnungen

IP-Adresse	MAC-Adresse	Hostname	Zuordnung verfällt (local time d/m/y)
192.168.1.192	00:0c:29:ca:01:05		~~15/01/2006 23:04:21~~
192.168.1.194	00:0c:29:b5:5a:60		~~14/01/2006 14:55:18~~
192.168.1.195	00:0c:29:1c:c3:ab		~~24/12/2005 00:00:07~~
192.168.1.196	00:0c:f1:24:bf:b3		~~27/12/2005 10:52:34~~
192.168.2.199	00:11:85:1e:78:ac		~~04/01/2006 22:59:29~~
192.168.2.200	00:0c:f1:24:bf:b3		~~28/12/2005 17:21:43~~

Anmerkung

Dieser Abschnitt wird *nur* dargestellt, wenn DHCP aktiviert ist. Siehe Abschnitt DHCP Server

2.3.2.3. Einträge in der Routing-Tabelle



Einträge der Routing-Tabelle:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
[redacted]      0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
1.1.1.0         0.0.0.0         255.255.255.0   U     0      0        0 eth2
0.0.0.0         [redacted]      0.0.0.0         UG    0      0        0 ppp0
```

2.3.2.4. Einträge in der ARP-Tabelle

Einträge der ARP-Tabelle:

```
Address                 HWtype  HWaddress           Flags Mask            Iface
192.168.1.52            ether   [redacted]          C                     eth0
```

2.3.3. System-Diagramme

Klicken Sie auf eines der vier Diagramme (CPU Diagramm, Memory Diagramm, Swap Diagramm oder Disk Diagramm), um Diagrammansichten für Tag, Woche, Monat und Jahr zu erhalten.

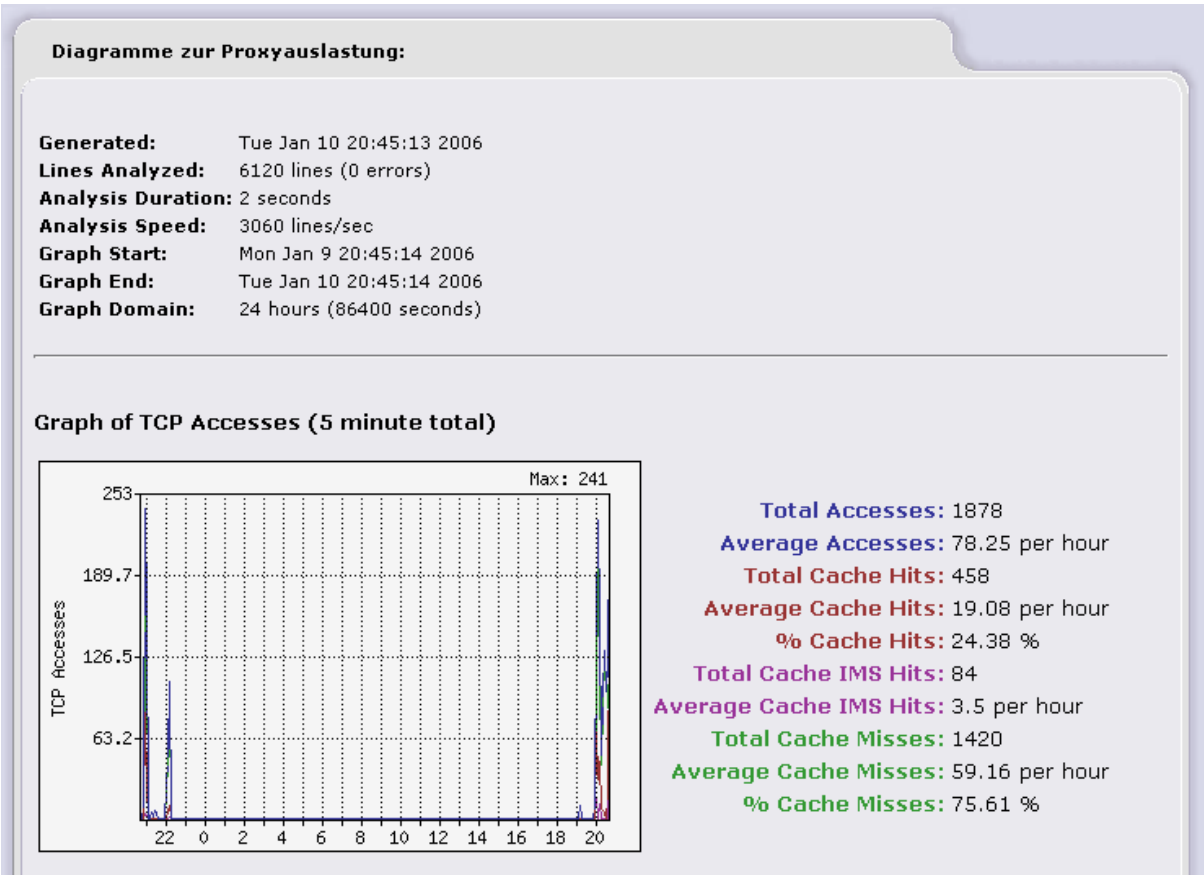
2.3.4. Netzwerk-Diagramme

Diese Seite gibt eine grafische Übersicht über den ein- und ausgehenden Netzwerk-Verkehr..

Für jede konfigurierte Netzwerk-Schnittstelle gibt es einen eigenen Abschnitt.

Klicken Sie auf eine der Grafiken, um Ansichten für Tag, Woche, Monat und Jahr zu erhalten.

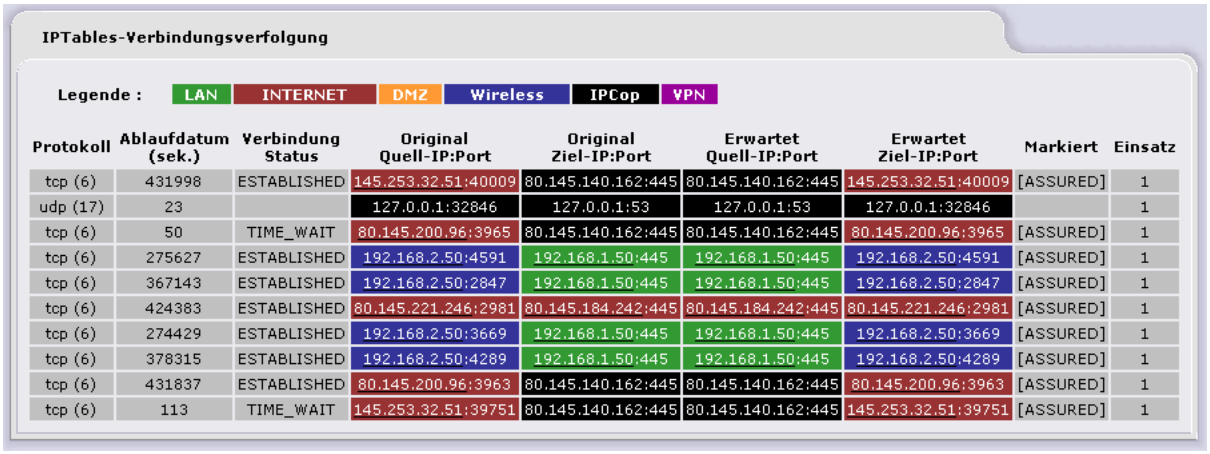
2.3.5. Proxy-Diagramme



Diese Seite zeigt den Datenverkehr durch den Proxy-Dienst des IPCops. Der erste Abschnitt zeigt Datum und Uhrzeit der Diagrammerstellung, die analysierten Verbindungen, die Dauer der Analyse, die Geschwindigkeit (Verbindungen pro Sekunde), Start- und Endzeit des Diagramms und die Domain (Gesamtlänge des Diagramms).

Diese Information ist nützlich, um zu sehen, ob der Proxy für die aufkommende Last korrekt konfiguriert ist.

2.3.6. IPTables Verbindungsverfolgung



Protokoll	Ablaufdatum (sek.)	Verbindung Status	Original Quell-IP:Port	Original Ziel-IP:Port	Erwartet Quell-IP:Port	Erwartet Ziel-IP:Port	Markiert	Einsatz
tcp (6)	431998	ESTABLISHED	145.253.32.51:40009	80.145.140.162:445	80.145.140.162:445	145.253.32.51:40009	[ASSURED]	1
udp (17)	23		127.0.0.1:32846	127.0.0.1:53	127.0.0.1:53	127.0.0.1:32846		1
tcp (6)	50	TIME_WAIT	80.145.200.96:3965	80.145.140.162:445	80.145.140.162:445	80.145.200.96:3965	[ASSURED]	1
tcp (6)	275627	ESTABLISHED	192.168.2.50:4591	192.168.1.50:445	192.168.1.50:445	192.168.2.50:4591	[ASSURED]	1
tcp (6)	367143	ESTABLISHED	192.168.2.50:2847	192.168.1.50:445	192.168.1.50:445	192.168.2.50:2847	[ASSURED]	1
tcp (6)	424383	ESTABLISHED	80.145.221.246:2981	80.145.184.242:445	80.145.184.242:445	80.145.221.246:2981	[ASSURED]	1
tcp (6)	274429	ESTABLISHED	192.168.2.50:3669	192.168.1.50:445	192.168.1.50:445	192.168.2.50:3669	[ASSURED]	1
tcp (6)	378315	ESTABLISHED	192.168.2.50:4289	192.168.1.50:445	192.168.1.50:445	192.168.2.50:4289	[ASSURED]	1
tcp (6)	431837	ESTABLISHED	80.145.200.96:3963	80.145.140.162:445	80.145.140.162:445	80.145.200.96:3963	[ASSURED]	1
tcp (6)	113	TIME_WAIT	145.253.32.51:39751	80.145.140.162:445	80.145.140.162:445	145.253.32.51:39751	[ASSURED]	1

IPCop benutzt die Linux Netfilter- und IPTables-Möglichkeiten, um als Firewall zu arbeiten. Firewalls überwachen Verbindungen zu und von allen Netzwer-IP-Adressen auf GREEN, BLUE und ORANGE, sowohl für Quell- und Zieladressen mit Ports, als auch den Status der Verbindung. Sobald eine Verbindung zwischen geschützten Maschinen aufgebaut wurde, dürfen nur noch Pakete die Firewall passieren, die konsistent zur Verbindung und dem aktuellen Status passen.

Das Fenster IPTables Verbindungsverfolgung zeigt die IPTables-Verbindungen. Verbindungen und Ziele sind entsprechend ihrer Netze farbcodiert. Die Legende zu den Farbcodes wird unten auf der Seite dargestellt.

Klicken Sie auf eine IP-Adresse, für einen Rückwärts-DNS-Lookup.

2.4. Netzwerk

2.4.1. Einwahl

Dieses Administrationsfenster ist in mehrere Bereiche aufgeteilt, dort können verschiedene Einstellungen vorgenommen werden. Diese Einstellungen sind nur nötig falls die Internetverbindung über ein analog Modem, über ISDN oder über einen DSL-Anschluss hergestellt wird.

Beachten Sie, dass Sie kein Profil auswählen oder ändern können solange die ROTE Schnittstelle des IPCop online ist (mit dem Internet verbunden ist) oder im Dial-On-Demand-Modus auf eine Verbindung wartet. Evtl. müssen Sie die Verbindung auf der Startseite erst Trennen. Nach einer Änderung am Profil können Sie den IPCop wieder über die Startseite Verbinden.

Profile . In diesem Bereich können Sie ein vorhandenes Einwahlprofil oder ein neues Profil auswählen. Insgesamt stehen 5 Profile zur Auswahl.

Das gewählte Profil können Sie bearbeiten oder Sie können es auswählen, um mit diesem Profil die Verbindung zum Internet aufzubauen. Möchten Sie aktuelle Änderungen (die noch nicht gespeichert wurden) rückgängig machen, können Sie das aktuelle Profil Wiederherstellen.

Verbindung . In diesem Bereich haben Sie folgende Möglichkeiten:

1. Wählen Sie die entsprechende Schnittstelle für das Gerät, welches Sie mit dem Internet verbinden soll.

Dies wird entweder ein serieller Anschluß sein (COM1 - COM4), welcher meist für Modems oder ISDN-Geräte benutzt wird oder PPPoE, welches hauptsächlich bei DSL-Verbindungen zum Einsatz kommt.

2. Wählen Sie die entsprechende Computer-zu-Modem Rate. Diese legt fest, mit welcher Geschwindigkeit Daten von und zu Ihrem Verbindungsgerät übertragen werden. Mit älteren Computern oder Modems kann es notwendig sein, eine niedrigere Übertragungsrate zu wählen, damit eine verlässliche Computer/Modem Verbindung hergestellt werden kann.

3. Geben Sie die korrekte Einwahlnummer für Ihre Internetverbindung ein. Wenn die Verbindung über PPPoE hergestellt wird, sollte dieses Feld im Normalfall leer bleiben.

4. Wählen Sie, ob der Modemlautsprecher ein- oder ausgeschaltet sein soll. Wenn er eingeschaltet ist, hören Sie, wie die Verbindung aufgebaut wird (dies kann auch für eine eventuelle Fehlersuche nützlich sein). Diese Option ist nur sinnvoll, wenn die Verbindung über ein analoges Modem erfolgt.

5. Legen Sie den Wahlmodus fest. Benutzen Sie möglichst Tonwahl, da dieses Verfahren gegenüber Pulswahl wesentlich schneller ist. Benutzen Sie nur Pulswahl, wenn Ihre Telefonverbindung nur dieses Verfahren unterstützt.

6. Geben Sie die Anzahl der Wählversuche an. Dies legt fest, wie oft IPCop versucht, sich nach einer fehlgeschlagenen Anwahl nochmals einzuwählen.

7. Geben Sie den Leerlauf-Timeout an. Dies legt fest, wie sich der IPCop verhält, wenn keine Daten über die Internetverbindung gesendet oder empfangen werden. Die hier eingegebene Zahl gibt an, wie lange IPCop nach der letzten Datenübertragung mit dem Trennen der Internetverbindung wartet. Wird dieser Parameter auf 0 gesetzt, trennt IPCop die einmal hergestellte Verbindung nicht mehr.

8. Der Radiobutton Dauerhaft#sorgt bei Aktivierung dafür, dass IPCop die Verbindung ständig aufrecht erhält, auch wenn kein Datenverkehr stattfindet. In diesem Modus wird die Internetverbindung nach jedem Abbruch (wie beispielsweise einem Verbindungs-Timeout) erneut aufgebaut. Nutzen Sie diesen Modus mit Bedacht. Wenn Sie einzelne Verbindungen berechnet bekommen, sollten Sie diesen Modus nicht benutzen. Sollten Sie hingegen eine Flatrate#haben, können Sie diese Option verwenden, um so lange wie möglich verbunden zu bleiben. Beachten Sie, dass IPCop in diesem Modus nach fehlgeschlagenen Verbindungen nach der eingestellten Anzahl von Wählversuchen aufhören wird sich zu verbinden. Sollte das eintreten, müssen Sie sich manuell auf der Startseite über den Anwahl-Schalter einwählen.

9. Dial-on-Demand kann über diesen Radiobutton aktiviert werden.

Anmerkung

Beachten Sie, daß der Anwahl-Schalter auf der Startseite einmal angeklickt werden muß, damit IPCop bei angeforderter Internet-Aktivität automatisch eine Verbindung herstellt.
Dial-on-Demand steht für PPPoE-Verbindungen nicht zur Verfügung.

10. Die Option Dial-on-Demand für DNS bestimmt, ob sich IPCop bei DNS-Anfragen automatisch einwählt. Dies ist normalerweise erwünscht.

11. Ist die Option Verbinden bei IPCop-Neustart aktiviert, verbindet sich der IPCop nach dem Starten sofort mit dem Internet (falls die Option Dial-on-Demand nicht aktiviert ist). Im Normalfall sollte diese Option aktiviert sein, wenn Dial-on-Demand eingestellt ist. Durch die Kombination dieser Optionen wird der IPCop beim Aktivieren oder Neustarten automatisch in den Dial-on-Demand Wartemodus gesetzt.

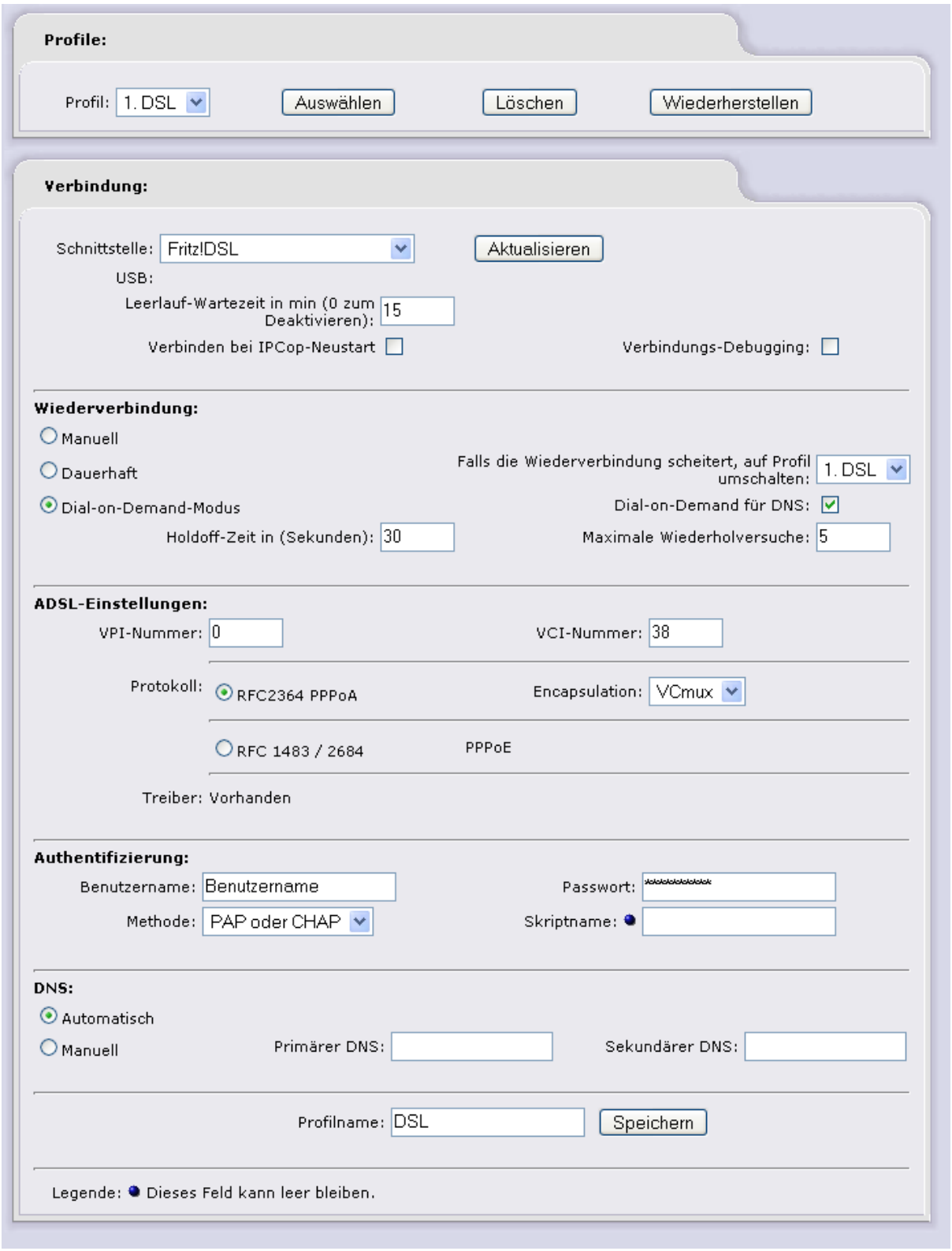
12. ISP erfordert Zeilenschaltung. Einige ISPs erfordern zwingend das Senden einer Zeilenschaltung vom Modem, welche das Ende einer Datenübertragung anzeigt. Sollte Ihr ISP dies erfordern, lassen Sie das Kontrollkästchen angehakt. Wenn nicht, können Sie den Haken entfernen. Standardmäßig ist diese Option eingeschaltet.

Zusätzliche PPPoE Einstellungen - Wenn PPPoE oder USB-ADSL aktiviert ist, sind zusätzliche Einstellmöglichkeiten verfügbar. Hier können Sie zwei zusätzliche Parameter eingeben: Einen Dienstnamen und einen Namen des VPN/der Firewall/des Gateways, welche manche ISPs verlangen. Sollte Ihr ISP dies nicht benötigen, oder Sie keine Informationen darüber bekommen haben, lassen Sie diese Felder leer.

Ihr ISP gibt Ihnen zwei Einstellungen: VPI und VCI, welche Sie eingeben müssen, wenn Sie USB-ADSL benutzen.

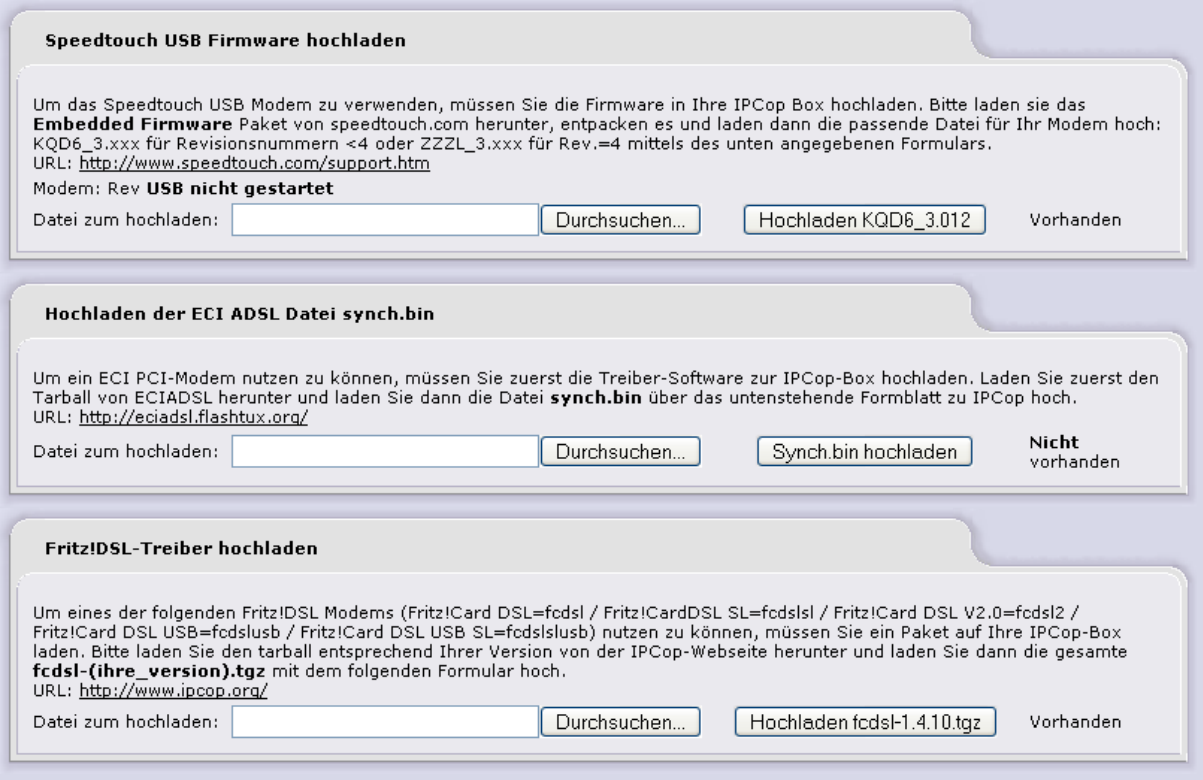
Authentifizierung. Hier müssen Sie den Benutzername und das Passwort eintragen, die Sie von Ihrem Provider erhalten haben. Es gibt verschiedene Möglichkeiten wie die Provider das Verbinden realisieren, die verbreitesten sind PAP und CHAP. Sollte Ihr Provider zum Verbinden ein textbasiertes Standard-Login-Skript oder ein anderes Skript verwenden, müssen Sie das hier angeben. Benötigen Sie ein anderes Skript, müssen Sie sich im IPCop-Computer einloggen und eine Datei in `/etc/ppp` erstellen. Den Dateinamen (ohne das `/etc/ppp`) müssen Sie in dem Textfeld Skriptname angeben. Die Datei muss „expect send“ Paare enthalten, jeweils getrennt durch ein Tab. *`USERNAME`* wird mit dem Benutzername und *`PASSWORD`* mit dem Passwort ersetzt. Als Beispiel können Sie sich die Datei `demonloginscript` in `/etc/ppp` anschauen oder als Vorlage verwenden.

DNS. Wählen sie Automatisch falls Sie die DNS Server automatisch von Ihrem Provider zugewiesen bekommen, dies ist das meistverbreiteste Vorgehen. Als Alternative können Sie die IP-Adressen von zwei DNS Servern manuell angeben. Normalerweise werden Ihnen diese Adressen von Ihrem Provider mitgeteilt.



2.4.2. Hochladen

Sie müssen verschiedene Dateien auf Ihren Arbeitsplatz-PC herunterladen. Diese Dateien sind nötig, um verschiedene Modems mit IPCop benutzen zu können. Über dieses Administrationsfenster können Sie die Dateien auf den IPCop hochladen, diese werden im IPCop installiert.



Speedtouch USB Firmware hochladen. Benutzen Sie diesen Bereich, um die Datei mgmt.o auf den IPCop hochzuladen. USB ADSL wird erst funktionieren wenn Sie die Datei hochgeladen haben. Benutzen Sie den angegebenen Link, registrieren Sie sich und laden Sie die Datei au Ihren Arbeitsplatz-PC herunter. Wählen Sie als nächstes die heruntergeladene Datei aus und benutzen Sie den Hochladen-Knopf, um die Datei auf den IPCop zu übertragen. Sobald Sie die Datei auf den IPCop übertragen haben, können Sie USB ADSL benutzen.

Hochladen der ECI ADSL Datei synch.bin. Benutzen Sie diesen Bereich, um die Datei sync.bin auf den IPCop hochzuladen. ECI ADSL wird erst funktionieren wenn Sie die Datei hochgeladen haben. Benutzen Sie den angegebenen Link und laden Sie die Datei auf Ihren Arbeitsplatz-PC herunter. Wählen Sie als nächstes die heruntergeladene Datei aus und benutzen Sie den Hochladen-Knopf, um die Datei auf den IPCop zu übertragen. Sobald Sie die Datei auf den IPCop übertragen haben, können Sie ECI ADSL benutzen.

Fritz!DSL-Treiber hochladen. Benutzen Sie diesen Bereich, um die Datei fcdsl.o auf den IPCop hochzuladen. Fritz!DSL wird erst funktionieren wenn Sie die Datei hochgeladen haben. Benutzen Sie den angegebenen Link und laden Sie die Datei auf Ihren Arbeitsplatz-PC herunter. Wählen Sie als nächstes die heruntergeladene Datei aus und benutzen Sie den Hochladen-Knopf, um die Datei auf den IPCop zu übertragen. Sobald Sie die Datei auf den IPCop übertragen haben, können Sie Fritz!DSL benutzen.

2.4.3. Modem

Modem Konfiguration. Diese ist nur notwendig wenn Sie sich mit einem Standard Analog Modem in das Internet einwählen. Die Standard Einstellungen, im Adminstrationsfenster, passen für die meisten Analog Modems. Sollten Sie Probleme mit diesen Einstellungen haben, dann sollten Sie die Einstellungen mit den benötigten Einstellung für Ihr Modem vergleichen. Zu finden sind die benötigten Einstellungen im Handbuch ihres Modems. Möglicherweise können oder müssen die Einstellungen auch leer sein.

Initialisierung - Die standard Initialisierung, die von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Sollte Ihr Modem andere Einstellungen benötigen, dann müssen Sie sie hier eintragen bzw. die Vorbelegung abändern.

Auflegen - Der standard Wert zum Auflegen, der von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Sollte Ihr Modem einen anderen Wert benötigen, müssen Sie diesen eintragen.

Lautsprecher ein - Der standard Wert zum Einschalten der Lautsprecher, der von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Sollte Ihr Modem einen anderen Wert benötigen,

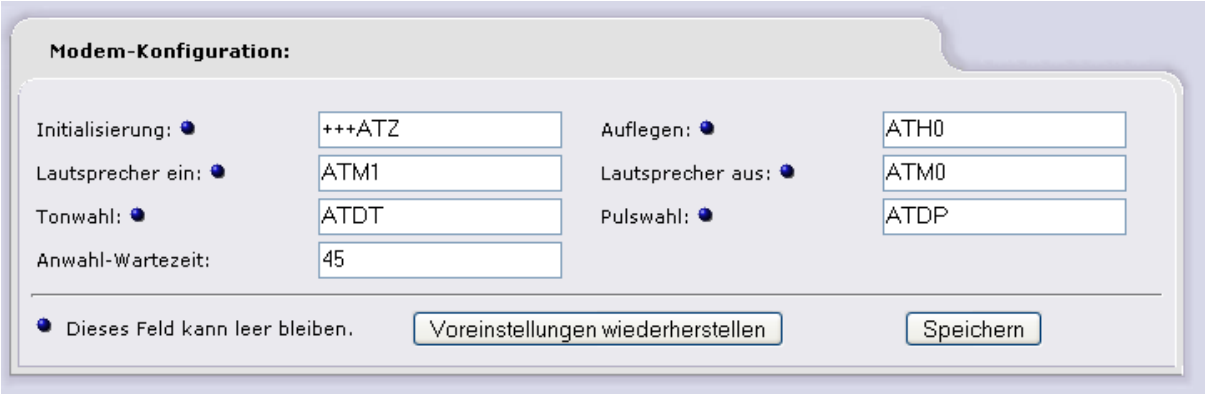
müssen Sie diesen eintragen.

Lautsprecher aus - Der standard Wert zum Ausschalten der Lautsprecher, der von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Sollte Ihr Modem einen anderen Wert benötigen, müssen Sie diesen eintragen.

Tonwahl - Der standard Tonwahl-Wert, der von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Falls Ihr Modem oder Ihr Telefonanschluss die Tonwahl unterstützen, sollten Sie bei Problemen mit der Tonwahl prüfen oder der eingetragene Wert für Ihr Modem richtig ist. Gegebenenfalls müssen Sie den Wert abändern.

Pulswahl - Der standard Pulswahl-Wert, der von den meisten Hayes-Kompatiblen Modems benutzt wird, ist bereits eingetragen. Normalerweise müssen Sie diesen Wert nicht ändern. Falls ihr Telefonanschluss aber keine Tonwahl unterstützt bzw. anbietet, sollten Sie prüfen, ob der eingetragene Wert für Ihr Modem richtig ist.

Die Anwahl-Wartezeit ist das einzige Feld, das nicht leer sein darf. Hier wird die Zeit eingetragen, die das Modem maximal Zeit hat sich zu verbinden. Ist nach der angegebenen Zeit noch keine Verbindung zustande gekommen, bricht IPCop diesen Versuch ab und startet einen neuen Verbindungsversuch. Normalerweise sollte der standard Wert ausreichen, sollten Sie jedoch feststellen, dass der Verbindungsversuch mitten in der Verhandlung mit der Gegenstelle abgebrochen wird, sollten Sie den Wert solange erhöhen bis die Verbindung erfolgreich aufgebaut werden konnte. Um festzustellen, ob während der Verhandlungsphase abgebrochen wird, stellen Sie am besten die Lautsprecher des Modems an und achten auf die Signaltöne beim Verbindungsversuch.



2.4.4. Externe Aliase

Anmerkung

Dieses Administrationsfenster ist nur über das Menü verfügbar wenn die ROTE Schnittstelle STATISCH konfiguriert ist.

Möglicherweise werden Ihnen von Ihrem Internetdienstanbieter mehrere IP-Adressen zugewiesen.

Wurden Ihnen diese zusätzlichen IP-Adressen ausschließlich zugewiesen, damit Sie auch von weiteren Clientcomputern aus auf das Internet zugreifen können, benötigen Sie diese IP-Adressen nicht mehr, denn Sie können von diesen Computern aus über den IPCop eine Verbindung zum Internet herstellen. In diesem Fall benötigen Sie lediglich einen Anschluss, über den der IPCop-Computer mit dem Internet verbunden wird.

Sollten Sie jedoch auf einem der internen Computer einen Server betreiben, können Sie die zusätzlichen IP-Adressen als Alias-Adressen an der ROTEN Schnittstelle benutzen. Um diese Möglichkeit tatsächlich nutzen zu können, müssen Sie eventuell die Routingtabelle des IPCop von Hand anpassen.

Sobald Sie die vollständigen Informationen eingetragen haben, setzen Sie das Häkchen hinter Aktiviert und klicken Hinzufügen. Die neue Alias-Adresse wird hierdurch zu den aktuellen Alias-Adressen (im unteren Bereich) hinzugefügt.

Aktuelle Alias-Adressen. In diesem Bereich sind die zurzeit eingetragenen Alias-Adressen aufgelistet. Um eine Alias-Adresse zu löschen müssen Sie das „Mülleimer"-Symbol anklicken. Um eine Alias-Adresse zu bearbeiten, benutzen sie das gelbe „Stift"-Symbol.

Zum de-/aktivieren einer Alias-Adresse müssen Sie das „Aktiviert"-Symbol (das Häkchen links in der „Aktion"-Spalte), der jeweiligen Adresse, anklicken. Das Häkchen im Symbol verschwindet und die Adresse ist deaktiviert. Um die Adresse wieder zu aktivieren, müssen Sie das leere Kästchen anklicken.

2.5. Dienste

IPCop bietet neben seiner zentralen Funktion als Internet-Firewall eine Reihe weiterer Dienste zur Verwendung in kleinen Netzwerken.

Diese lauten wie folgt:

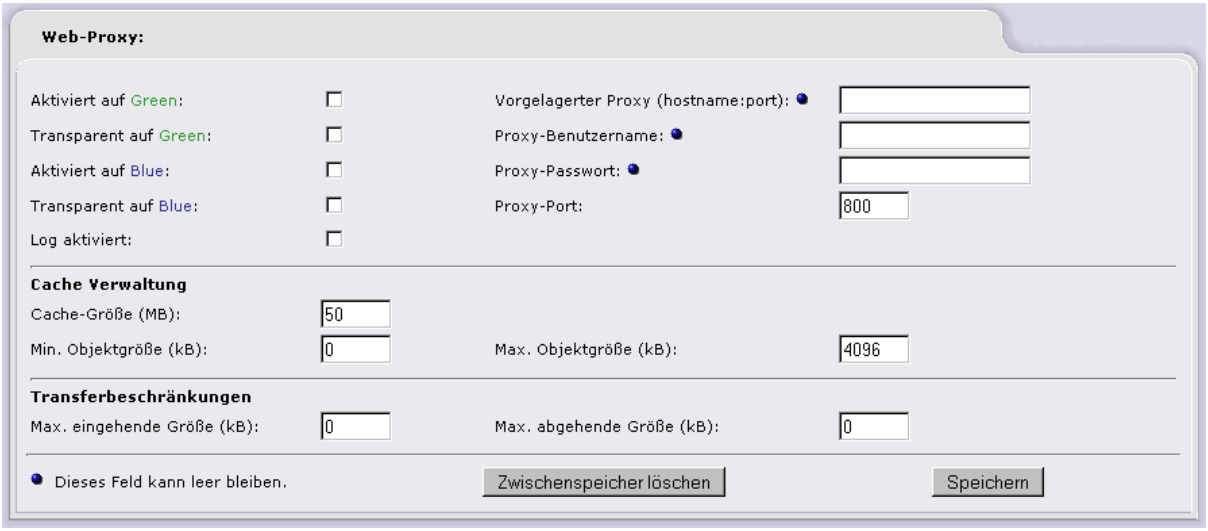
- Proxy (Internet-Proxyserver)
- DHCP Server
- Verwaltung für dynamische DNS
- Hosts bearbeiten (Lokaler DNS-Server)
- Zeitserver
- Traffic Shaping
- Einbruchdetektierung

In größeren Netzwerken werden diese Dienste möglicherweise von dedizierten Servern bereitgestellt oder ihre Verwendung ist nicht erforderlich. In diesem Fall sollten die entsprechenden Dienste in IPCop deaktiviert werden.

2.5.1. Proxy

Bei einem Web-Proxyserver handelt es sich um ein Programm, dass stellvertretend für alle anderen Computer in Ihrem Intranet Anfragen nach Webseiten durchführt. Der Proxyserver speichert die aus dem Internet abgerufenen Seiten zwischen, sodass beispielsweise in dem Fall, dass drei Computer im Intranet dieselbe Seite anfordern, diese lediglich einmal aus dem Internet abgerufen werden muss. Wenn in Ihrer Organisation auf bestimmte Websites von mehreren Benutzern häufiger zugegriffen wird, kann auf diese Weise der Internetzugriff reduziert werden.

In der Regel müssen die Webbrowser in dem lokalen Netzwerk dafür konfiguriert werden, für den Internetzugriff einen Proxyserver zu verwenden. Wenn Sie den IPCop-Proxy verwenden, sollten Sie für den Namen bzw. die Adresse des Proxyservers im Browser den IPCop-Computer angeben. Für den Port (Anschluss) sollten Sie den Wert angeben, der im Feld Proxy-Port eingetragen ist (Standardwert: 800). Diese Konfiguration ermöglicht den Benutzern bei Bedarf den Proxyserver zu umgehen. Daneben besteht die Möglichkeit, den Proxyserver in einem sog. "transparenten" Modus auszuführen. In diesem Fall benötigen die Browser keine besondere Konfiguration, und die Firewall leitet das gesamte Datenaufkommen auf Port 80, dem Standard-HTTP-Port, auf den Proxyserver um.



Sie können auswählen, ob Anfragen von dem grünen (privaten) oder von dem blauen (WLAN-) Netzwerk über den Proxyserver erfolgen sollen. Aktivieren Sie einfach die entsprechenden Kontrollkästchen.

Wenn Sie den Proxyserver einsetzen, können Sie auch die Zugriffe auf das Internet protokollieren, indem Sie das Kontrollkästchen Log aktiviert aktivieren. Sie können die Internetzugriffe über den Proxyserver einsehen, indem Sie im Menü Logs den Befehl Proxy-Logdateien wählen.

Wenn bei Ihrem Internetdienstanbieter die Verwendung seines Zwischenspeichers für den Internetzugriff erforderlich ist, geben Sie den Hostnamen und den Port im Textfeld Vorgelagerter Proxy ein. Ist für die Verwendung des Proxyservers Ihres Internetdienstanbieters die Angabe eines Benutzernamens bzw. Kennworts erforderlich, geben Sie geben Sie diese Informationen in den Textfeldern Proxy-Benutzername bzw. Proxy-Kennwort ein.

Cacheverwaltung. In diesem Bereich können Sie festlegen, wie viel Speicherplatz auf der Festplatte für die Zwischenspeicherung von Webseiten bereitgestellt werden soll. Darüber hinaus können Sie auch die Größe des kleinsten (standardmäßig 0 KB) bzw. größten (standardmäßig 4096 KB) zwischenzuspeichernden Objektes festlegen. Aus Gründen des Datenschutzes erfolgt durch den Proxyserver keine Zwischenspeicherung von Webseiten, die über https empfangen werden, oder bei denen Benutzername und Kennwort über den URL übermittelt werden.

Transferbeschränkungen. Der Internet-Proxyserver kann auch zur Steuerung des Internetzugriffs durch die Benutzer im Intranet genutzt werden. Die einzig mögliche Steuerung über die Web-Benutzeroberfläche ist die Größenbeschränkung der vom und zum Internet übermittelten Daten gegeben. Durch Verwendung dieser Optionen können Sie verhindern, dass Benutzer umfangreiche Dateien downloaden und auf diese Weise die Geschwindigkeit des Internetzugriffs der anderen Benutzer beeinträchtigen. Legen Sie für den Wert 0 (dies ist die Standardeinstellung) fest, um alle Beschränkungen aufzuheben.

Klicken Sie auf Speichern, um die Änderungen zu speichern.

Sie können jederzeit alle zwischengespeicherten Seiten aus dem Proxy-Cache löschen, indem Sie auf die Schaltfläche Zwischenspeicher löschen klicken.

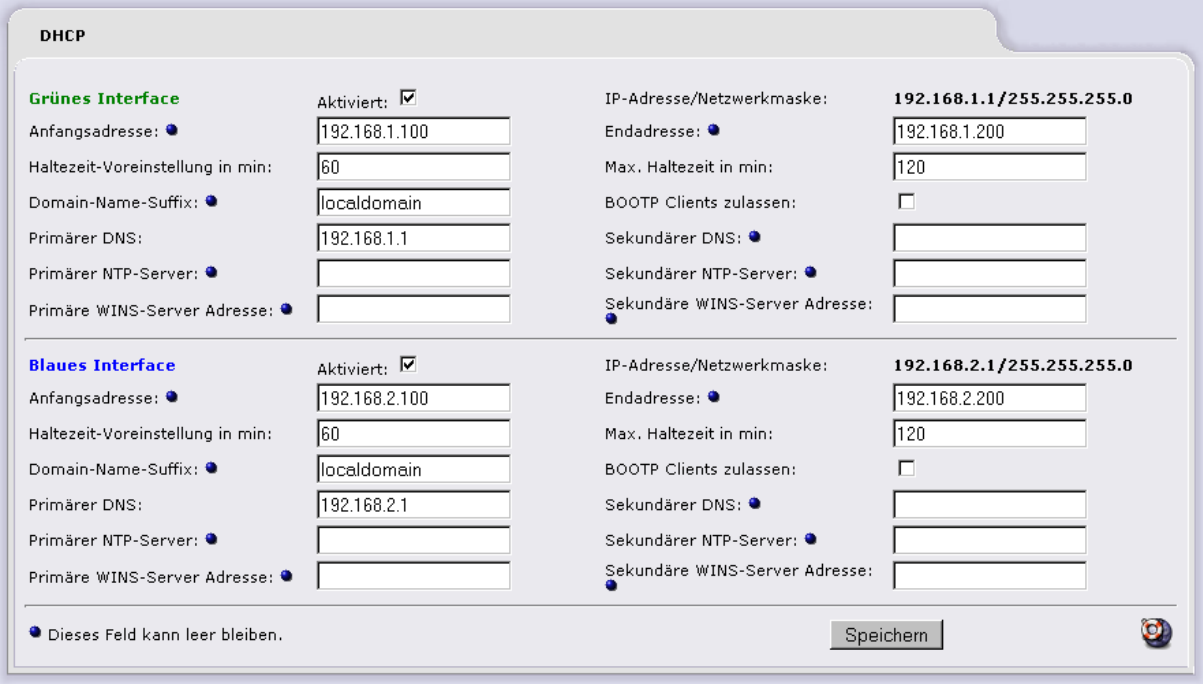
Warnung

Zwischengespeicherte Dateien können umfangreiche Mengen an Speicherplatz belegen. Wenn Sie dem Proxyserver für das Zwischenspeichern von Internetseiten viel Speicherplatz beimessen, ist möglicherweise die in der Dokumentation zu IPCop angegebene Minimalanforderung für den Festplatten-Speicherplatz nicht ausreichend.

Je größer der festgelegte Zwischenspeicher ist, desto mehr Arbeitsspeicher benötigt der Proxyserver auch für die Verwaltung des Zwischenspeichers. Wenn Sie IPCop auf einem Computer mit geringem Speicherausbau ausführen, sollten Sie den Zwischenspeicher nicht zu groß machen.

2.5.2. DHCP

DHCP (Dynamic Host Configuration Protocol) ermöglicht eine Steuerung der Netzwerkkonfiguration aller Computer über den IPCop-Computer. Computern, die eine Verbindung zum Netzwerk herstellen, wird eine gültige IP-Adresse zugewiesen, und ihre DNS- und WINS-Konfiguration wird von dem IPCop-Computer festgelegt. Um diese Funktion verwenden zu können, müssen die Computer im Netzwerk so konfiguriert sein, dass sie ihre Netzwerkkonfiguration automatisch erhalten.



Sie können auswählen, ob Sie diesen Dienst dem grünen (privaten) Netzwerk oder dem blauen (WLAN-) Netzwerk zur Verfügung stellen möchten. Aktivieren Sie einfach die entsprechenden Kontrollkästchen.

Eine umfassende Erläuterung der Konzepte zu DHCP finden Sie in dem folgenden Artikel in englischer Sprache aus Linux Magazine: „Network Nirvana - How to make Network Configuration as easy as DHCP“ [http://www.linux-mag.com/2000-04/networknirvana_01.html]

2.5.2.1. DHCP-Server-Parameter

Über die Web-Benutzeroberfläche können die folgenden DHCP-Parameter festgelegt werden:

Aktiviert	Markieren Sie dieses Feld, um den DHCP-Server für dieses Netzwerk zu aktivieren.

IP Addresse/Netzwerkmaske — Die IP-Adresse des Netzes und die Netzmaske werden hier zur Übersicht dargestellt.

Anfangsadresse (optional) — Sie können die unterste und die oberste Adresse angeben, die der Server für andere Computern bereitstellt. Standardmäßig werden die Adressen dem gesamte Teilnetzbereich entnommen, das bei der Installation von IPCop angegeben wurde. Wenn sich in Ihrem Netzwerk Computer befinden, die DHCP nicht verwenden, deren IP-Adressen also manuell festgelegt werden, sollten Sie Anfangs- und Endadresse so wählen, dass der DHCP-Server keine dieser manuell vergebenen IP-Adressen vergibt.

Sie sollten darüber hinaus sicherstellen, dass sich auch keine der im Bereich Aktuelle feste Zuordnungen angegebenen Adressen (siehe unten) in diesem Bereich befinden.

Endadresse (optional) — Gibt die oberste Adresse der zu vergebenden Adressen an (siehe oben).

Anmerkung

Wenn Sie die Start- und Endadresse leer lassen, werden keine dynamischen Adressen vergeben. Wenn Sie eine Startadresse angeben, müssen Sie auch eine Endadresse angeben.

Haltezeit-Voreinstellung — Verwenden Sie den Vorgabewert, wenn Sie keinen triftigen Grund haben, einen anderen Wert zu verwenden. Die Haltezeit-Voreinstellung ist die Zeitdauer in Minuten, die IP-Adress-Leasen vorgehalten werden. Vor dem Ablauf der Lease (der Zeitpunkt, zu dem die zugewiesene IP-Adresse verfällt) fordern Clientcomputer unter Angabe ihrer aktuell gültigen IP-Adresse eine Erneuerung der Lease an. Bei einer Anforderung auf e ine Erneuerung der Lease werden ggf. durchgeführte Änderungen an DHCP-Parametern berücksichtigt, und die Clientkonfiguration wird entsprechend aktualisiert. Im Allgemeinen werden IP-Adresszuordnungen vom Server erneuert.

Maximale Vorhaltezeit — Verwenden Sie den Vorgabewert, wenn Sie keinen triftigen Grund haben, einen anderen Wert zu verwenden. Die maximale Vorhaltezeit ist das Zeitintervall (in Minuten) während der der DHCP-Server Clientanfragen auf Erneuerung der Lease für die aktuell gültige IP-Adresse immer zustimmt. Nach Ablauf der maximalen Vorhaltezeit kann die IP-Adresse des Clients vom Server geändert werden. Wenn der Bereich des Pools für die Vergabe von IP-Adressen (der dynamische IP-Adressbereich) zwischenzeitlich geändert wurde, erhält der Client eine neue IP-Adresse aus dem neuen dynamischen IP-Adressbereich.

Domain-Name-Suffix (optional) — Achten Sie bei der Eingabe eines Wertes in dieses Textfeld darauf, dass das Format keinen führenden Punkt (.) vorsieht. Legt den Domänennamen fest, den der DHCP-Server für seine Clients verwendet. Wenn ein Hostname nicht aufgelöst werden kann, versucht der Client erneut, den ursprünglichen Namen mit dem als Namen angegeben Suffix aufzulösen. Die DHCP-Server von vielen Internetdienstanbietern sind so konfiguriert, dass als Standarddomänename deren Netzwerk verwendet wird, und sie fordern ihre Kunden auf, beim Internetzugriff "www" als Standard-Homepage in ihrem Browser festzulegen. "www" ist jedoch kein vollqualifizierter Domänenname (FQDN). Der vollqualifizierte Domänenname des Webservers wird jedoch automatisch clientseitig über die Software Ihres Computers erstellt, indem das Suffix des Domänennamens wie von dem DHCP-Server des Internetdiensanbieters vorgegeben angehängt wird. Legen Sie das Domänen-Name-Suffix entsprechend der Vorgabe des DHCP-Servers Ihres Internetdiensanbieters fest, damit die Benutzer in Ihrem Intranet weiterhin die Teiladresse "www" nicht eingeben müssen.

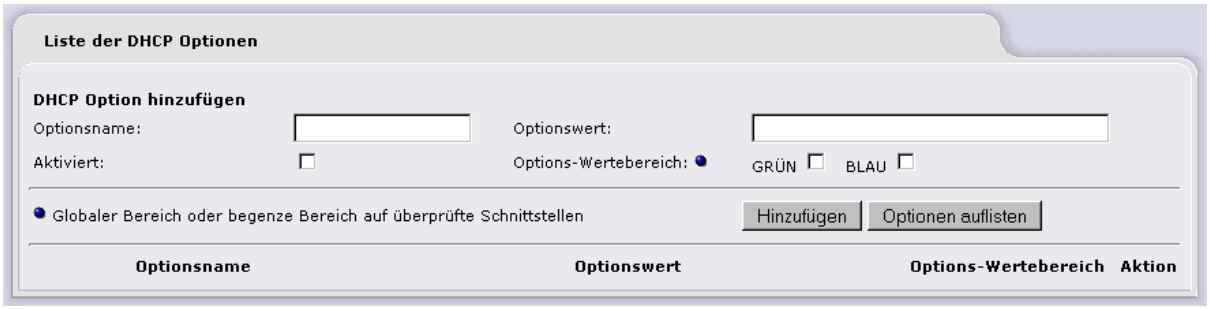
BOOTP Clients zulassen — Markieren Sie dieses Feld, um BOOTP Clients Leases in diesem Netz-

	werk zuzuweisen. Standardmässig ignoriert IPCop Bootstrap Protocol (BOOTP) Pakete.
Primärer DNS	Legt für die Clients des DHCP-Servers fest, welcher Server als primärer DNS-Server verwendet werden soll. Da IPCop auch einen DNS-Proxy enthält, wird in der Regel empfohlen, den Standardwert zu verwenden. In diesem Fall wird für den primären DNS-Server die IP-Adresse des IPCop-Computers verwendet. Wenn Sie einen eigenen separaten DNS-Server verwenden, geben Sie dessen IP-Adresse in das Feld ein.
Sekundärer DNS (optional)	Sie können auch einen sekundären DNS-Server angeben, der verwendet wird, falls der primäre DNS-Server nicht verfügbar sein sollte. Dieser DNS-Server könnte beispielsweise ein weiterer DNS-Server in Ihrem Netzwerk oder der DNS-Server Ihres Internetdienstanbieters sein.
Primärer NTP Server (optional)	Wenn Sie IPCop als NTP-Server einsetzen, oder die Adresse eines anderen NTP-Servers an Geräte in Ihrem Netzwerk weiterleiten wollen, können Sie die IP-Adresse des NTP-Servers in dieses Feld eingeben. Der DHCP-Server gibt diese Adresse an alle Clients weiter, wenn Sie ihre Netzwerkparameter erhalten.
Sekundärer NTP Server (optional)	Wenn Sie eine zweite NTP-Server-Adresse haben, geben Sie diese hier ein. Der DHCP-Server wird die Adresse an alle Clients weitergeben, wenn Sie ihre Netzwerkparameter erhalten.
WINS-Server Adresse (optional)	Wenn Ihr Netzwerk auch ein Windows-Netzwerk umfasst und Sie einen WINS-Server (Windows Naming Service-Server) verwenden, können Sie in diese Felder den primären bzw., falls vorhanden, sekundären WINS-Server eintragen. Der DHCP-Server übergibt diese Adresse an die Hostcomputer, wenn diese ihre Netzwerkparameter erhalten.

Nach dem Klicken auf Speichern werden die Änderungen übernommen.

2.5.2.2. Liste der DHCP Optionen

Wenn Sie weitere spezielle Parameter über den DHCP-Server an Ihr Netzwerk übergeben wollen, können Sie diese hier eintragen.



Hier können Sie zusätzliche DHCP Optionen hinzufügen:

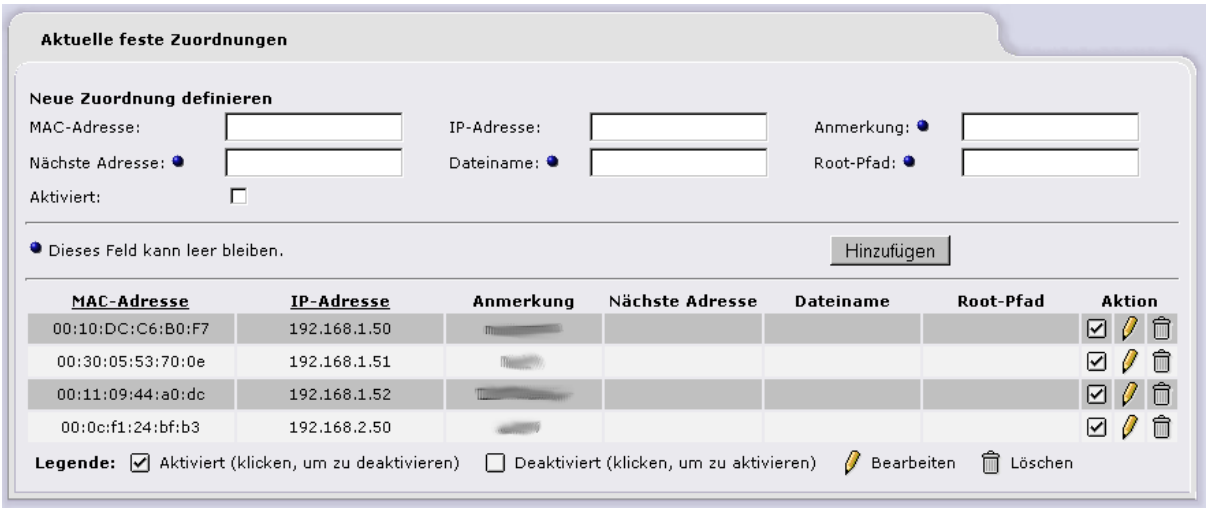
Optionsname	Der Name der DHCP Option, z.B.: `smtp-server` oder `tcp-keepalive-interval`.
Optionswert	Der Wert der zugehörigen Option. Dabei kann es sich um einen Text, einen Zahlenwert, eine IP-Adresse usw. handeln.
Options-Wertebereich (optional)	Der Wertebereich der Option wird global, solange keine der Boxen hier markiert ist. In diesem Fall gilt die Option nur für die markierten Netzbereiche.

Aktiviert	Wenn dieses Feld markiert ist, wird die Option aktiviert, andernfalls werden die Einstellungen gespeichert, aber nicht benutzt.
Hinzufügen	Über diesen Schalter wird die neue Option angelegt.
Optionen auflisten	Klicken Sie auf diesen Schalter, um eine Liste der Optionen mit passenden Werten zu erhalten.

2.5.2.3. Neue Zuordnung definieren

Wenn sich in Ihrem Netzwerk Computer befinden, deren IP-Adressen zentral verwaltet werden sollen, für die es jedoch darüber hinaus auch erforderlich ist, dass sie stets dieselbe IP-Adresse erhalten, können Sie über den DHCP-Server festlegen, dass diesen Computern auf der Grundlage der MAC-Adresse der in dem Computer installierten Netzwerkkarte eine feste IP-Adresse zugewiesen wird.

Diese Art der Konfiguration unterscheidet sich wesentlich von der manuellen Adresszuweisung, da auch diese Computer weiterhin ihre IP-Adressen von dem DHCP-Server beziehen. Die Adressen werden also nicht manuell auf dem Computer selber, sondern zentral über den DCHP-Server vergeben.



Für feste Zuordnungen können die folgenden Parameter festgelegt werden:

MAC-Addresse	Die sechs Oktett/Byte lange MAC-Adresse (in Doppelpunktnotation) des Computers, für den die feste Zuordnung gelten soll.

Warnung

Das Format der MAC-Adresse lautet xx:xx:xx:xx:xx:xx, und nicht xx-xx-xx-xx-xx-xx, wie es auf einigen Computern angezeigt wird (Beispiel: 00:e5:b0:00:02:d2).

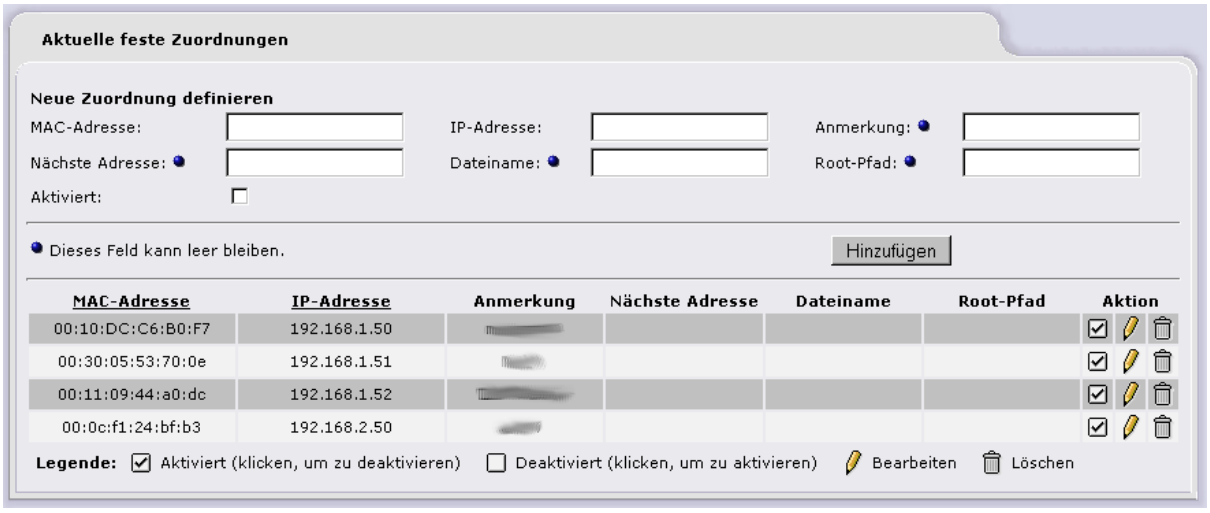
IP-Addresse	Die fest zugeordnete IP-Adresse, die der DHCP-Server stets für die angegebene MAC-Adresse vergeben soll. Stellen Sie sicher, dass Sie keine IP-Adresse aus dem dynamischen Adressbereich des DHCP-Servers vergeben.
Anmerkung (optional)	Hier können Sie einen beschreibenden Text für die feste Zuordnung vergeben.
Nächste Addresse (optional)	Möglicherweise befinden sich in Ihrem Netzwerk Computer, die eine Startdatei von einem Server im Netzwerk erhalten müssen (sog. Thin Clients). Für diese können Sie bei Bedarf in diesem Feld den die Serveradresse angeben.

Dateiname (optional)	Geben Sie den Namen der Startdatei für diesen Computer an.
Root-Pfad (optional)	Wenn sich die Startdatei nicht im Stammverzeichnis des Servers befindet, können Sie in diesem Feld den Pfad zu der Startdatei angeben.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, um den DHCP-Server anzuweisen, die angegebene feste Zuordnung bereitzustellen. Ist das Kontrollkästchen nicht deaktiviert, wird der entsprechende Datensatz in den Dateien von IPCop gespeichert, der DHCP-Server gibt die Zuordnung jedoch nicht aus.

2.5.2.4. Aktuelle feste Zuordnungen

In diesem Bereich werden die aktuellen festen Zuordnungen angezeigt und können bearbeitet oder gelöscht werden.

Sie können die Liste sortieren, indem Sie auf die unterstrichenen Spaltenüberschriften *MAC-Adresse* oder *IP-Adresse* klicken. Ein weiterer Klick dreht die Sortierreihenfolge um.



Zum Bearbeiten einer bestehenden festen Zuordnung klicken Sie auf das zugehörige Stift-Symbol. Die Werte für die feste Zuordnung werden im Ausschnitt Neue Zuordnung definieren auf der Seite angezeigt. Die feste Zuordnung wird in der Liste der festen Zuordnungen nicht mehr angezeigt. Der Datensatz für die feste Zuordnung ist verloren, bis Sie im Ausschnitt Neue Zuordnung definieren auf die Schaltfläche Speichern klicken. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf Speichern.

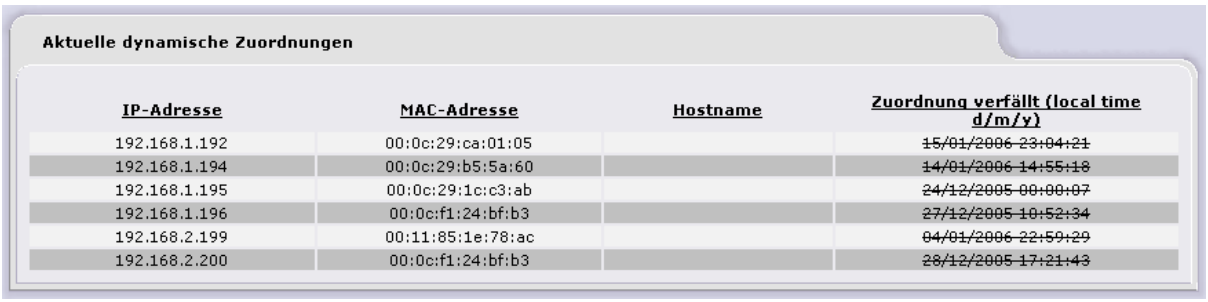
Zum Löschen einer bestehenden festen Zuordnung klicken Sie auf das zugehörige Papierkorb-Symbol. Die feste Zuordnung wird gelöscht.

2.5.2.5. Aktuelle dynamische Zuordnungen

Ist DHCP aktiviert, werden in diesem Bereich die aktuellen dynamischen Zuordnungen aus der Datei `/var/state/dhcp/dhcpd.leases` angezeigt. Es werden die IP-Adresse, die MAC-Adresse, der Hostname (falls verfügbar) und die Ablaufzeit der Lease für alle in dieser Datei aufgeführten Datensätze, sortiert nach der IP-Adresse, angezeigt.

Sie können die Liste umsortieren, indem Sie auf eine der unterstrichenen Spaltenüberschriften klicken. Ein weiterer Klick dreht die Sortierreihenfolge um.

Die Anzeige ermöglicht bei Bedarf das problemlose Kopieren einer MAC-Adresse, um sie in den Abschnitt-Neue Zuordnung definieren einzufügen.



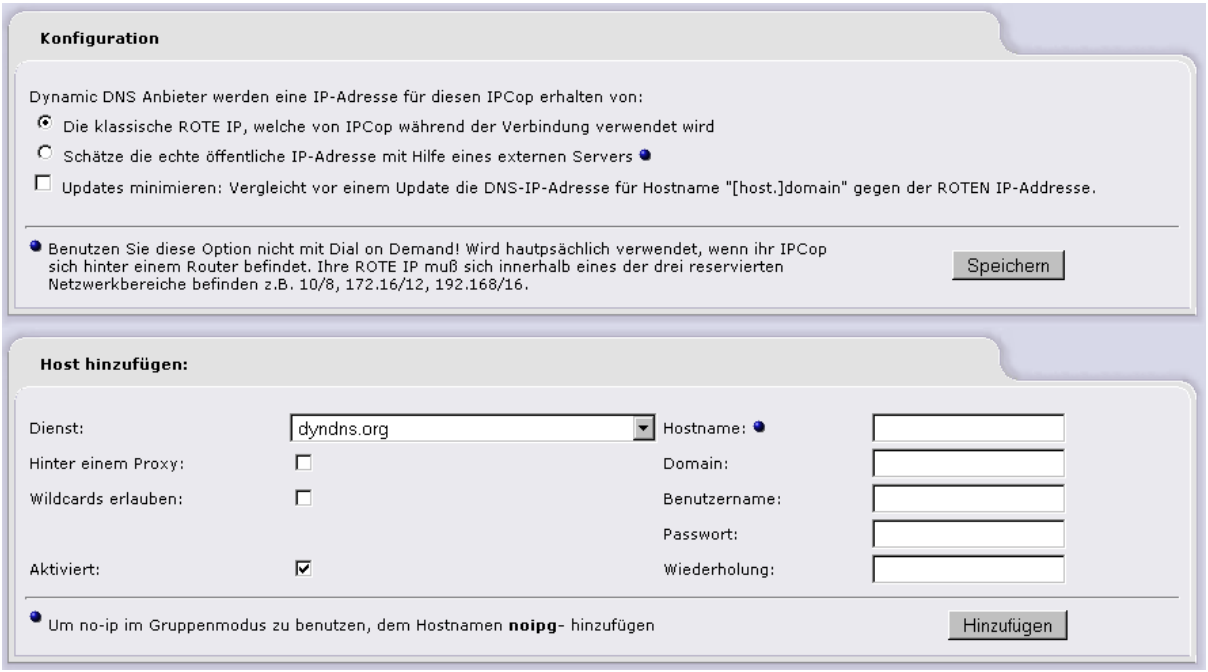
Leasen, die bereits abgelaufen sind, werden „durchgestrichen“ angezeigt.

2.5.2.6. Fehlermeldungen

Wenn nach dem Klicken auf die Schaltfläche Speichern ein Fehler in den Eingabedaten gefunden wird, wird oben auf der Seite eine Fehlermeldung angezeigt.

2.5.3. Dynamischer DNS

Mithilfe dynamischer DNS (DYNDNS) können Sie einen Server im Internet verfügbar machen, auch wenn dieser über keine statische öffentliche IP-Adresse verfügt. Um DYNDNS verwenden zu können, müssen Sie zunächst bei einen DYNDNS-Anbieter eine Unterdomäne registrieren. Anschließend muss Ihr Server jedes Mal, wenn eine Verbindung zum Internet herstellt und ihm von Ihrem Internetdienstanbieter eine IP-Adresse zugewiesen wird, dem DYNDNS-Server diese IP-Adresse mitteilen. Hostcomputer, die eine Verbindung zu Ihrem Server herstellen möchten, lösen die Adresse über den DYNDNS-Server auf, der die aktuellste gültige IP-Adresse bereitstellt. Ist diese IP-Adresse aktuell, kann der Hostcomputer eine Verbindung zu Ihrem Server herstellen (vorausgesetzt, die festgelegten Firewall-Regeln lassen dies zu). IPCop unterstützt die fortlaufende Aktualisierung Ihrer DYNDNS-Adresse durch die automatische Aktualisierung bei zahlreichen DYNDNS-Anbietern.



2.5.3.1. Host hinzufügen

Über die Web-Benutzeroberfläche können die folgenden DYNDNS-Parameter festgelegt werden:

Dienst — Wählen Sie einen DYNDNS-Anbieter aus der Dropdownliste aus. Sie sollten bei dem ausgewählten Anbieter bereits registriert sein.

Hinter einem Proxy	Aktivieren Sie dieses Kontrollkästchen nur dann, wenn Sie als Anbieter "no-ip.com" gewählt haben, und der Computer unter IPCop sich hinter einem Proxyserver befinden. Dieses Kontrollkästchen wird bei Auswahl eines anderen Anbieters nicht berücksichtigt.
Wildcards erlauben	Wenn Sie Platzhalterzeichen zulassen, ermöglichen Sie, dass alle Unterdomänen Ihres dynamischen DNS-Hostnamens auf dieselbe IP-Adresse wie Ihr Hostname selbst verweisen. Ist das Kontrollkästchen aktiviert, erhält beispielsweise die Unterdomäne www.ipcop.dyndns.org dieselbe IP-Adresse wie die übergeordnete Domäne ipcop.dyndns.org. Wenn Sie als Anbieter "no-ip.com" gewählt haben, wird das Kontrollkästchen nicht berücksichtigt, da dieser Anbieter die Einstellung dieser Option ausschließlich über seine Website ermöglicht.
Hostname	Geben Sie den Hostnamen ein, den Sie bei Ihrem DYNDNS-Anbieter registriert haben.
Domain	Geben Sie den Domänennamen ein, den Sie bei Ihrem DYNDNS-Anbieter registriert haben.
Benutzername	Geben Sie den Benutzernamen ein, den Sie bei Ihrem DYNDNS-Anbieter registriert haben.
Passwort	Geben Sie das Kennwort für den Benutzernamen ein.
Aktiviert	Aktivieren Sie dieses Kontrollkästchen, damit IPCop die auf dem DYNDNS-Server hinterlegten Daten aktualisiert. Die Daten werden auch auf dem IPCop-Computer gespeichert, wenn das Kontrollkästchen deaktiviert ist. Auf diese Weise können Sie die DYNDNS-Aktualisierung zu einem späteren Zeitpunkt wieder aktivieren, ohne die Daten erneut eingeben zu müssen.

2.5.3.2. Aktuelle Hosts

In diesem Bereich werden die aktuell konfigurierten DYNDNS-Einträge angezeigt.

Zum Bearbeiten einer Eintrags klicken Sie auf das zugehörige Stift-Symbol. Die Daten des Eintrags werden in dem Formular darüber angezeigt. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf die Schaltfläche Speichern auf dem Formular.

Die Kontrollkästchen Hinter einem Proxy, Wildcards erlauben und Aktiviert können auch direkt in der Liste der aktuellen Hosts aktiviert bzw. deaktiviert werden.

2.5.3.3. Erzwingen einer manuellen Aktivierung

Sie eine Aktualisierung der auf dem DYNDNS-Server hinterlegten Daten über IPCop erzwingen, indem Sie auf die Schaltfläche Aktualisierung erzwingen klicken. Es wird jedoch empfohlen, nur dann die Aktualisierung zu erzwingen, wenn sich die IP-Adresse tatsächlich geändert hat, da die Aktualisierung ohne tatsächliche Änderungen auf der Seite des DYNDNS-Anbieter vermeidbaren Aufwand bedeutet. Nach dem Aktivieren der Hosteinträge wird die zugehörige IP-Adresse bei jeder Änderung automatisch aktualisiert.

2.5.4. Hosts bearbeiten

Der in IPCop integrierte DNS-Proxy ermöglicht neben der Zwischenspeicherung von DNS-Informationen aus

dem Internet auch die manuelle Eingabe von Hostcomputern, deren Adressinformationen lokal verwaltet werden sollen. Bei diesen Hostcomputern kann es sich beispielsweise um lokale Computer oder Computer im Internet, deren Adressinformationen überschrieben werden sollen.

2.5.4.1. Host hinzufügen

Über die Web-Benutzeroberfläche können die folgenden Parameter festgelegt werden:

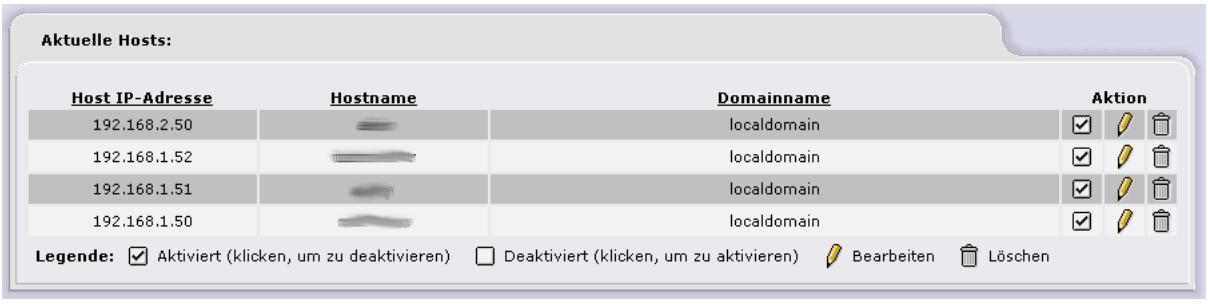
Host IP-Addresse	Geben Sie die in dieses Feld die IP-Adresse ein.
Hostname	Geben Sie in dieses Feld den Hostnamen ein.
Domainname (optional)	Geben Sie in dieses Feld den Domänennamen ein, falls sich der Hostcomputer in einer anderen Domäne befindet.
Aktiviert	Markieren Sie dieses Feld, um den Eintrag zu aktivieren Check this box to enable the entry.

Durch Klicken auf die Schaltfläche Hinzufügen wird der Eintrag gespeichert.

2.5.4.2. Aktuelle Hosts

In diesem Bereich werden die aktuell konfigurierten lokalen DNS-Einträge angezeigt.

Sie können die Liste sortieren, indem Sie auf eine der drei unterstichenen Spaltenüberschriften klicken. Ein weiterer Klick dreht die Sortierreihenfolge um.



Um einen Eintrag zu aktiviern oder zu deaktivieren, klicken Sie auf das „Aktiviert“-Symbol.

Zum Bearbeiten einer Eintrags klicken Sie auf das zugehörige Stift-Symbol. Die Daten des Eintrags werden in dem Formular darüber angezeigt. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf die Schaltfläche Speichern auf dem Formular.

Zum Löschen eines Eintrags klicken Sie auf das zugehörige Papierkorb-Symbol.

2.5.5. Zeitserver

IPCop kann so konfiguriert werden, dass die Uhrzeit mit einem als bekannten genauen Zeitserver im Internet abgeglichen wird. Darüber hinaus besteht die Möglichkeit, die auf diese Weise erhaltene genaue Uhrzeit für die anderen Computern im Netzwerk bereitzustellen.

Stellen Sie zur Konfiguration des Zeitsynchronisierungssystems sicher, dass das Kontrollkästchen Uhrzeit von einem Netzwerk Zeitserver ermitteln aktiviert ist, und geben Sie den vollständigen Namen des zu verwendenden Zeitservers in das Feld Primärer NTP-Server ein. Bei Bedarf können Sie auch einen Sekundärer NTP-Server angeben.

Wenn Sie den Zeitsynchronisierungsdienst auch dem internen Netzwerk zur Verfügung stellen möchten, aktivieren Sie das Kontrollkästchen Uhrzeit dem lokalen Netzwerk zur Verfügung stellen.

Sie können festlegen, dass die Uhrzeit auf dem Computer unter IPCop regelmäßig aktualisiert wird, beispielsweise stündlich, oder sie nur bei Bedarf manuell über diese Webseite aktualisieren (klicken Sie dazu einfach auf die Schaltfläche Stelle jetzt die Uhrzeit ein).

Klicken Sie auf die Schaltfläche Speichern, um die Konfiguration zu speichern.

Anmerkung

IPCop kann zwar als Zeitserver für Ihr Netzwerk eingesetzt werden, verwendet jedoch das Programm ntpupdate, um die Uhrzeit in regelmäßigen Abständen zu aktualisieren, anstelle des genaueren ntpd-Servers, der eine fortlaufende Synchronisierung der Uhrzeit ermöglicht. Dies bedeutet, dass die Uhrzeit auf dem IPCop-Computer mit höherer Wahrscheinlichkeit von der tatsächlichen Uhrzeit abweicht, es ist jedoch nicht erforderlich, dass der Computer permanent mit dem Internet verbunden ist.

Wenn Sie keinen Internet-Zeitserver verwenden möchten, können Sie Datum und Uhrzeit manuell eingeben, und dann auf die Schaltfläche Sofortiges Update klicken.

Warnung

Wenn Sie die Uhrzeit um einen großen Wert verändern, kann es passieren, dass der fcron-Server, der zeitgesteuerte Jobs startet, nicht mehr arbeitet. Dies wirkt sich dann auf die Erstellung der Diagramme und andere regelmässige Jobs aus, die im Hintergrund laufen.

Wenn dies passiert, versuchen Sie den fcron-Server mit dem Kommando **fcrontab -z** neu zu starten.

2.5.6. Traffic Shaping

Traffic Shaping, also die Optimierung der Datenübertragung, ermöglicht die Festlegung von Vorrangregeln für die verschiedenen IP-Datenströme, die durch die Firewall geleitet werden. IPCop setzt für diesen Zweck WonderShaper ein. WonderShaper ist hinsichtlich der Minimierung der Ping-Latenzzeit konzipiert, und stellt sicher,

dass für interaktive Datenübermittlung wie SSH bei gleichzeitiger Aufrechterhaltung des Dauerdatenverkehrs in beiden Richtungen genügend Bandbreite zur Verfügung steht.

Viele Internetdienstanbieter verstehen unter Übertragungsgeschwindigkeit die Downloadübertragungsrate, und nicht die Latenzzeit. Sie konfigurieren Ihre Geräte so, dass für Ihr Datenaufkommen umfangreiche Warteschlangen vorgehalten werden, um auf diese Weise die Downloadrate zu erhöhen. Wenn diese Warteschlangen auch interaktives Datenaufkommen enthalten, geht die Latenzzeit stark nach oben, da die ACK-Pakete in Ihrer Position in der Warteschlange verbleiben, bis sie "frei" werden, und an Sie übermittelt werden können. Mit IPCop erhalten Sie eine Möglichkeit, die Übertragungsverfahren des Datenaufkommens selbst Ihren Bedürfnissen entsprechend zu optimieren. Die Steuerung erfolgt durch die Einstufung des Datenaufkommens in Prioritätsstufen "Hoch", "Mittel" und "Niedrig". Die Ping-Übertragung erhält stets die höchste Priorität, damit Sie auch dann die Geschwindigkeit Ihrer Verbindung genau überprüfen können, während umfangreiche Downloads aus dem Internet durchgeführt werden.

So verwenden Sie die Traffic Shaping-Funktionalität in IPCop:

1. Verwenden Sie Ihnen bekannte schnelle Sites, um die maximalen Upload- und Downloadgeschwindigkeiten zu ermitteln. Geben Sie die so ermittelten Geschwindigkeiten in die entsprechenden Felder im Bereich Einstellungen der Webseite ein.

2. Aktivieren die Übertragungsoptimierung, indem Sie das Kontrollkästchen Aktivieren aktivieren.

3. Ermitteln Sie, welche Dienste in Ihrem Netzwerk verwendet werden, bei denen Datenübertragungen über die Firewall vom bzw. ins Internet erfolgen.

4. Weisen Sie diesen die gewünschte Priorität zu. Beispiel:

    a. Interaktivem Datenaufkommen wie SSH (Port 22) und VoIP wird die Prioritätsstufe „Hoch“ zugeordnet.

    b. Standarddatenaufkommen wie Browsen (Port 80) und Kommunikation (beispielsweise E-Mail-Verkehr über Port 25 bzw. 110) sowie Audio- und Videostreaming wird die Prioritätsstufe „Mittel“ zugeordnet.

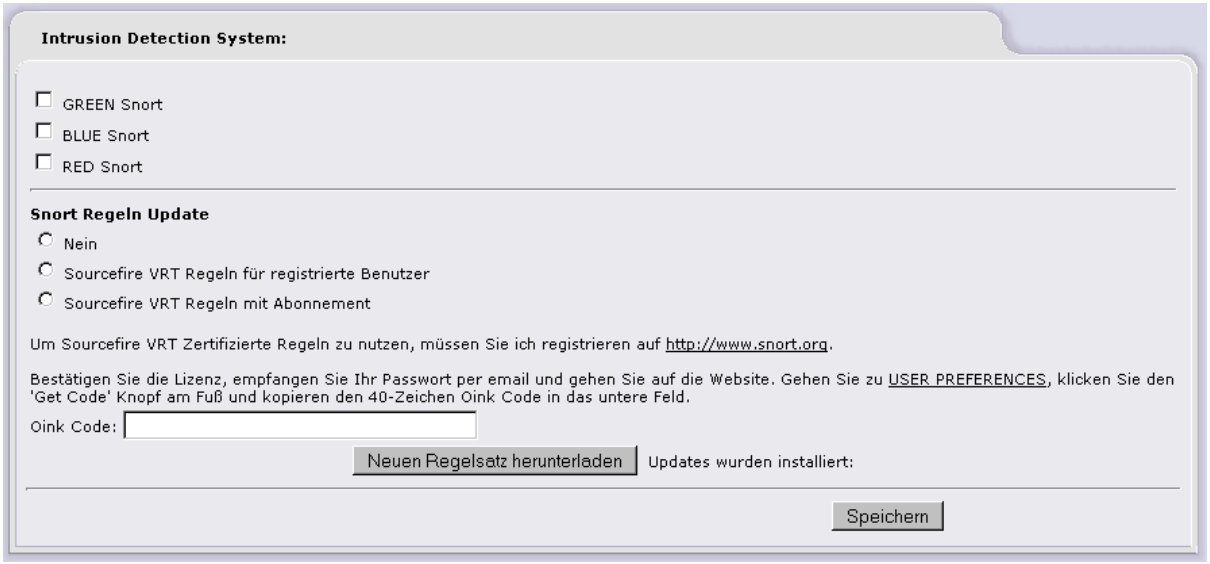
    c. Dauerdatenübertragungen wie beispielsweise P2P-Dateifreigaben erhalten die Prioritätsstufe „Niedrig“.

5. Erstellen Sie im Bereich Dienst hinzufügen der Webseite eine Liste mit Diensten und jeweils zugeordneten Prioritätsstufen.

Die oben genannten Dienste sind lediglich Beispiele für mögliche Konfigurationen zur Optimierung der Übertragung des Datenaufkommens. Sie sollten die Einstufung in die drei Prioritätskategorien entsprechend den Anforderungen in Ihrem Netzwerk anpassen.

2.5.7. Einbruchdetektierung

IPCop enthält ein hochleistungsfähiges System zur Einbruchserkennung, Snort, das die von der Firewall empfangenen IP-Pakete analysiert, und nach bekannten Signaturen für schädliche Aktivitäten durchsucht.



IPCop kann IP-Pakete überwachen, die über das rote, das grüne und das blaue Netzwerk übertragen werden. Aktivieren Sie einfach die gewünschten Kontrollkästchen, und klicken Sie auf Speichern.

2.5.7.1. Snort Regeln Update

Da fortlaufend neue Formen des Angriffs von außen bekannt werden, werden die Regeln, auf deren Grundlage Snort sie erkennt, ebenfalls fortlaufend aktualisiert. Klicken Sie auf die Schaltfläche Neuen Regelsatz herunterladen, um die neueste Version downzuloaden.

2.6. Firewall

Unter dem Menüpunkt Firewall werden einige der Kernfunktionalitäten des IPCop Servers zur Steuerung des Datenflusses duch die Firewall bereitgestellt.

Diese sind:

- Port Weiterleitung
- Externer Zugang (Erlaubt die Fernwartung des IPCop über das Internet)
- DMZ-Schlupflöcher
- Zugriff auf BLAU (Einen WLAN Access Point am IPCop betreiben)
- Firewall Optionen

2.6.1. Welcher Datenverkehr ist zwischen den Schnittstellen erlaubt?

Die untentstehende Tabelle fasst die Standardeinstellungen der Firewall zusammen und beschreibt die Schritte, die nötig sind, Zugriffe zwischen den Schnittstellen zu öffnen und zu verwalten.

Rot	⇨	Firewall	Geschlossen, benutzen Sie externen Zugang
Rot	⇨	Orange	Geschlossen, benutzen Sie Port-Weiterleitung
Rot	⇨	Blau	Geschlossen, benutzen Sie Port-Weiterleitung oder VPN
Rot	⇨	Grün	Geschlossen, benutzen Sie Port-Weiterleitung oder VPN
Orange	⇨	Firewall	Geschlossen (benutzen Sie IPCop nicht als DNS oder DHCP-Server für Orange)
Orange	⇨	Rot	Offen
Orange	⇨	Blau	Geschlossen, benutzen Sie DMZ-Schlupflöcher
Orange	⇨	Grün	Geschlossen, benutzen Sie DMZ-Schlupflöcher
Blau	⇨	Firewall	Geschlossen, benutzen Sie Zugriff auf Blau
Blau	⇨	Rot	Geschlossen, benutzen Sie Zugriff auf Blau
Blau	⇨	Orange	Geschlossen, benutzen Sie Zugriff auf Blau
Blau	⇨	Grün	Geschlossen, benutzen Sie DMZ-Schlupflöcher oder VPN
Grün	⇨	Firewall	Offen
Grün	⇨	Rot	Offen
Grün	⇨	Orange	Offen
Grün	⇨	Blau	Offen

2.6.2. Benutzer-Einstellungen

Seit Version 1.4 gibt es eine neue Datei, in der benutzerdefinierte Einstellungen zu den Firewall-Regeln abgelegt werden: `/etc/rc.d/rc.firewall.local`

Diese Datei wird durch `/etc/rc.d/rc.firewall` verarbeitet. Der manuelle Aufruf erfolgt durch:

```
$ /etc/rc.d/rc.firewall.local {start|stop|reload}
```

Anmerkung

Die **reload** Option wurd in Version 1.4.2 hinzugefügt und in Version 1.4.6 erweitert. Diese Änderungen sind in den offiziellen Updates nicht enthalten, um zu verhindern, dass benutzerdefinierte Einstellungen überschrieben werden.

Es existieren auch zwei spezielle Regelketten, die für benutzerspezifische Anpassungen vorgesehen sind: `CUSTOMINPUT`, `CUSTOMFORWARD`. Diese Regelketten existieren seit Version 1.3.

Ebenfalls seit Version 1.3 existiert die Datei `/etc/rc.d/rc.local`, die beim Systemstart ausgeführt wird. In dieser Datei können benutzerspezifische Kommandos eingepflegt werden, die beim Booten erforderlich sind (z.B. Initialisierung eines internen Modems).

Keine dieser Dateien wird durch ein offizielles Update verändert. Die Dateien werden mitgesichert, wenn die IPCop-Datensicherung ausgeführt wird.

2.6.3. Port-Weiterleitung

Über diese Seite werden die Port-Weiterleitungen verwaltet. Port-Weiterleitungen sind zu 100% optional, Sie können dieses Kapitel also überspringen, wenn Sie von diesem Feature keinen Gebrauch machen wollen.

2.6.3.1. Übersicht

Firewalls blockieren von extern gestellte Anfragen vor dem geschützten System. Manchmal kann diese Einstellung zu restriktiv sein. Wenn Sie z.B. einen Webserver betreiben, würden alle von ausserhalb des geschützten Netzwerks kommenden Benutzeranfragen standardmässig blockiert. Dies würde bedeuten, dass der Webserver nur aus dem internen Netz zu nutzen wäre. Dies ist natürlich nicht die Normalsituation für einen Webserver. Die meisten Leute **möchten** Aussenstehenden den Zugriff auf ihren Webserver ermöglichen. Für diese Fälle gibt es Port-Weiterleitungen.

Port-Weiterleitung ist ein Dienst, der von aussen begrenzten Zugriff auf das interne LAN ermöglicht. Wenn Sie Ihren Webserver einrichten, können Sie die Ports wählen, auf denen der Webserver „lauscht“. Diese Einstellung hängt von der verwendeten Software ab, ziehen Sie also ggf. die Dokumentation der Webserver-Software zu Rate.

Wenn diese Ports fertig eingerichtet sind, können Sie die Port-Weiterleitung im IPCop konfigurieren. Über die TCP/UDP Liste wird das verwendete Protokoll für die Weiterleitungsregel festgelegt. Die meisten Server verwenden TCP, einige Spiele- und Chatserver verwenden UDP. Wenn das Protokoll in der Server-Dokumentation nicht angegeben ist, handelt es sich für gewöhnlich um TCP. Quell-Port ist der Port, auf den von aussen verbunden wird. In den meisten Fällen wird dies der Standard-Port für den angebotenen Dienst sein (80 für Webserver, 20 für FTP-Server, 25 für Mailserver usw.). Sie können hier auch einen Port-Bereich angeben, indem Sie einen Doppelpunk „:“ zwischen die Portnummern setzen (niedrigste Portnummer zuerst). Ziel-IP-Adresse ist die interne IP-Adresse des Servers (z.B. 192.168.0.3). Ziel-Port ist der oben beschriebene Port, auf dem der Serverdienst lauscht. Über die Liste Alias-IP-Adresse können Sie festlegen, welche rote IP-Adresse von dieser Weiterleitung betroffen ist. IPCop kann mehr als eine rote IP-Adresse verwalten. Wenn Sie nur eine rote IP-Adresse haben, wählen Sie hier DEFAULT IP.

2.6.3.2. Port-Weiterleitung und externer Zugang

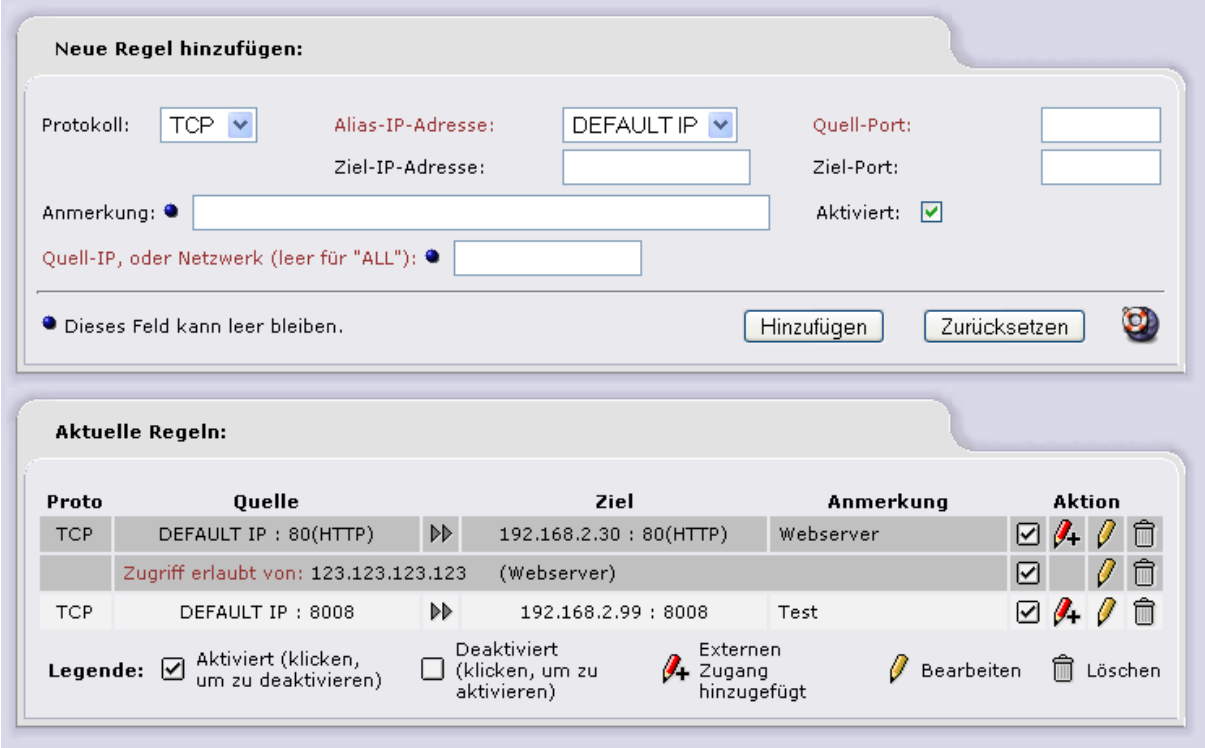
In Version 1.3.0 wurde das Interface zur Port-Weiterleitung überarbeitet. Es unterscheidet sich deutlich von älteren Versionen. Die oben beschriebenen Portnummern gelten aber weiterhin.

Die Seite Externer Zugang hat **keinen** Einfluss auf das grüne oder orangene Netzwerk. Sie dient dazu, Ports auf den IPCop selbst zu öffnen und nicht auf das grüne oder orangene Netzwerk.

Wie ermöglicht man dann den externen Zugang? Er ist kombiniert in der Port-Weiterleitungs-Seite - über das Feld

'Quell-IP, oder Netzwerk (Leer für "ALL"):'

Dieses Feld kontrolliert den externen Zugang - wenn Sie es leer lassen, wird die Port-Weiterleitung für **alle Internet-Adressen** geöffnet. Alternativ können Sie hier eine Adress oder Netzwerk eintragen, die Weiterleitung wird dann hierauf begrenzt.



Sie können mehr als eine externe Adresse haben. Nachdem Sie den Weiterleitungs-Eintrag angelegt haben, erscheint er in der Tabelle. Wenn Sie eine weitere externe Adresse hinzufügen möchten, klicken Sie auf den roten Bleistift mit dem Plus-Symbol. Der Eintrag wird in die Eingabefelder oben übernommen und Sie können eine neue IP-Adresse oder ein neues Netzwerk hinzufügen.

Nach dem Speicher taucht der neue Eintrag in der Tabelle auf.

Weiterhin muss beachtet werden:

- Das GRE-Protokoll wird unterstützt.
- Bei den Ports können Bereiche mit Platzhaltern (Wildcards) eingegeben werden. Einige Beispiele:
- * ergibt 1-65535
- 85-* ergibt 85-65535
- *-500 ergibt 1-500

Folgende Zeichen können bei der Angabe von Port-Bereichen verwendet werden: „:“ oder „-“. Beachten Sie, dass „-“ in „:“ übersetzt wird, auch wenn es als „-“ angezeigt wird.

Sie müssen nur den ersten Quell-Port eingeben, der Ziel-Port wird automatisch eingetragen.

Sie können einen Eintrag ändern, in dem Sie auf den gelben Bleistift in der jeweiligen Zeile klicken.

Wenn Sie einen Eintrag bearbeiten, wird er in der Tabelle gelb hervorgehoben.

Um einen Eintrag zu löschen, klicken Sie auf den Papierkorb.

Port-Bereiche dürfen sich nicht überlappen.

Einzelne Ports können nicht innerhalb von bereits vergebenen Port-Bereichen festgelegt werden. Wenn Sie z.B. den Bereich 2000-3000 vergeben haben, können Sie Port 2500 nicht mehr vergeben, Sie erhalten dann eine Fehlermeldung. Auch kann ein Port nicht auf mehrere Maschinen weitergeleitet werden.

Reservierte Ports - auf der roten Hauptadresse (DEFAULT IP) sind einige Ports für IPCop reserviert. Dies sind die Ports 67, 68, 81, 222 und 445.

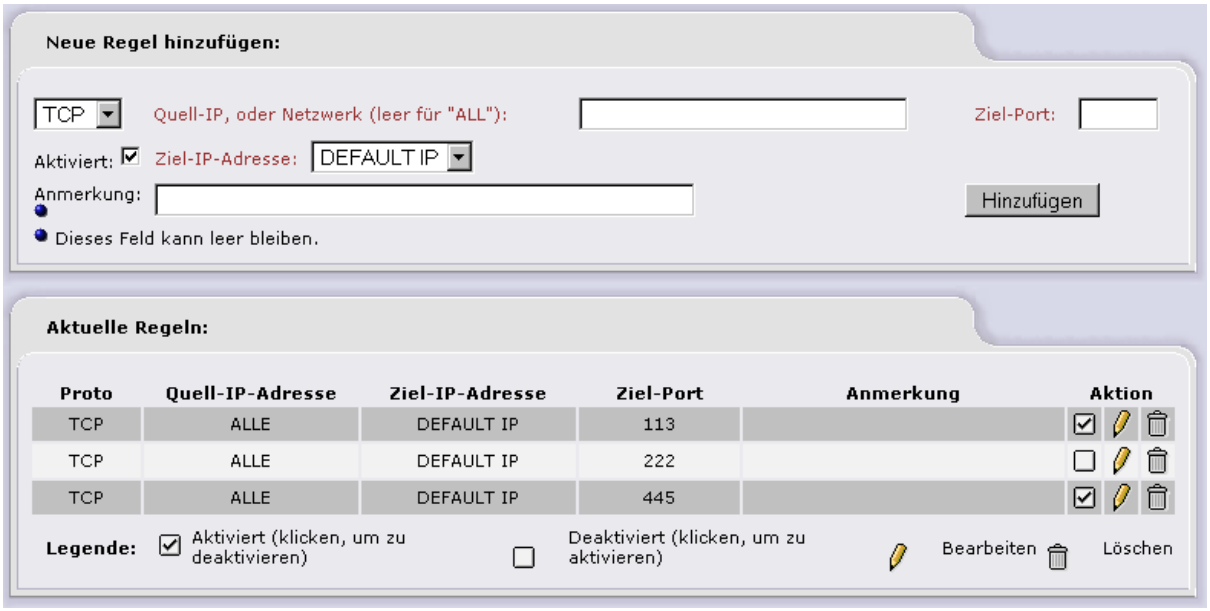
Wenn Sie eine Portweiterleitung bearbeiten, erscheint eine separate Checkbox 'Überschreibe externen Zugang zu ALL:'. Sie dient dazu, den Port für Testzwecke schnell für alle Internet-Adressen zu öffnen. Dieses Feature entstand aus einer Benutzer-Anforderung.

Beachten Sie, dass ein für mehrere externe Adressen geöffneter Port für alle Adressen geöffnet wird, wenn Sie die einzelnen Adressen löschen.

Mit einem Klick auf den Aktiviert-Schalter können Sie eine Weiterleitung schnell ein- und ausschalten. **Achtung:** Wenn Sie eine Port-Weiterleitung deaktivieren, werden alle zugewiesenen externen Adressen deaktiviert.

2.6.4. Externer Zugang

Über diese Seite können Sie den externen Zugang auf Ihren IPCop konfigurieren. Diese Einstellung ist optional, wenn Sie keinen externen Zugang zum IPCop benötigen, können Sie diesen Abschnitt überspringen.



Seit Version 1.3.0 wird über den externen Zugang nur der Zugriff auf den IPCop eingerichtet. Dies hat keinen Einfluss auf den Zugriff auf das grüne, blaue oder orangene Netz. Nutzen Sie dazu bitte die Port-Weiterleitung.

Wenn Sie Ihren IPCop fernwarten wollen, konfigurieren Sie den TCP-Port 445 (HTTPS). Wenn Sie auch ssh-Zugang von extern benötigen, konfigurieren Sie den TCP-Port 222 (SSH).

Über die Liste TCP/UDP wählen Sie das Protokoll für die Regel. Die meisten normalen Server benutzen TCP. Quell-IP ist die IP-Adresse des externen Rechners, dem Sie die Zugangsberechtigung geben wollen. Sie können dieses Feld leer lassen, damit ist der Zugriff für jede Adresse erlaubt. Dies kann eine Gefahrenquelle darstellen, ist aber nützlich, wenn Sie den IPCop von überall aus fernwarten wollen. Ziel-Port ist der externe Port, über den der Zugriff gestattet werden soll, z.B. 445. Über Ziel-IP-Adresse können Sie die IP-Adresse der roten Schnittstelle festlegen, für die die Regel gelten soll. IPCop kann mehrere IP-Adressen an der roten Schnittstelle verwalten. Wenn Sie nur eine rote IP-Adresse haben, wählen Sie hier DEFAULT IP.

Wenn alle Eingaben getätigt wurden, setzen Sie das Häkchen bei Aktiviert und klicken Sie Hinzufügen. Die Regel wird dann in die Tabelle unten aufgenommen.

Unter Aktuelle Regeln werden alle eingerichteten Zugangsregeln aufgelistet. Um eine Regel zu löschen, klicken Sie auf das Papierkorb-Symbol. Um einen Eintrag zu bearbeiten, klicken Sie auf das gelbe Bleistift-Symbol.

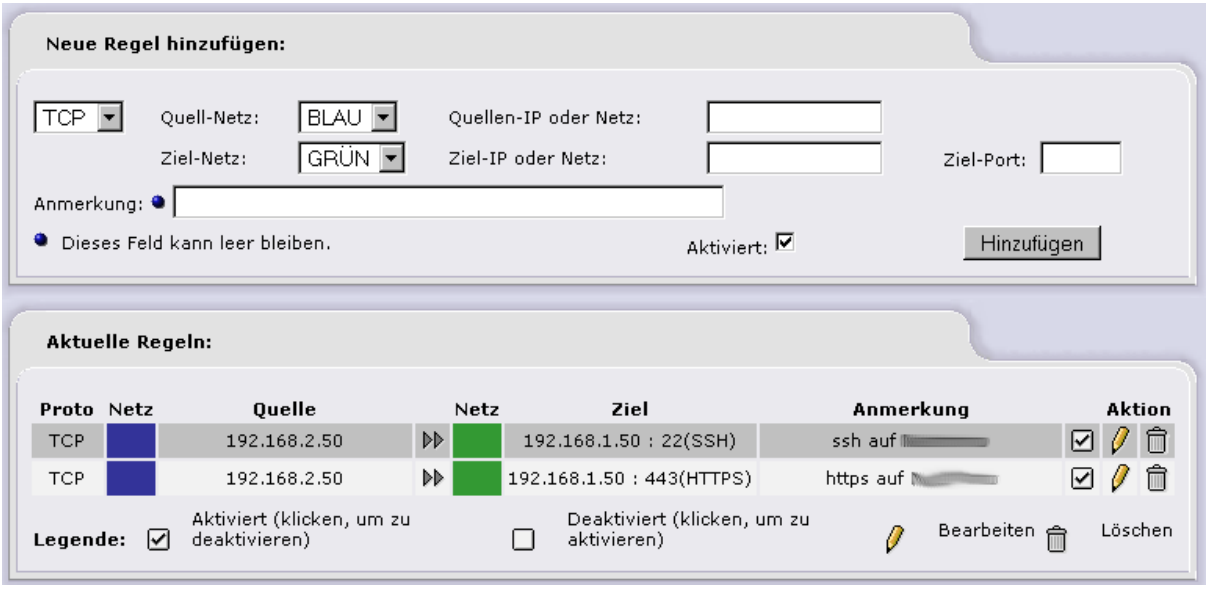
Um eine Regel schnell zu aktivieren oder deaktivieren, klicken Sie auf das Symbol mit dem Häkchen.

2.6.5. DMZ-Schlupflöcher

Über diese Seite konfigurieren Sie die DMZ-Schlupflöcher. Diese Einstellungen sind optional, wenn Sie keine Schlupflöcher benötigen, können Sie diesen Abschnitt überspringen.

Anmerkung

Diese Seite wird nur angezeigt, wenn Sie eine Netzwerkkarte für Blau oder Orange installiert haben.



Eine DMZ oder Demilitarisierte Zone (ORANGE Zone) wird als halbsicherer Austauschpunkt zwischen der externen ROTEN Zone und der internen GRÜNEN Zone genutzt. In der GRÜNEN Zone befinden sich alle Ihre internen Rechner. Die ROTE Zone ist das gesamte Internet. Eine DMZ ermöglicht es nun, Serverdienste anzubieten, ohne unzulässige Zugriffe auf das interne LAN durch Benutzer in der ROTEN Zone zu erlauben.

Nehmen wir an, Ihr Unternehmen betreibt einen Webserver. Sicherlich wollen Sie, daß Ihre Kunden (die in der ROTEN Zone) darauf zugreifen können. Weiterhin sei angenommen, daß Ihr Webserver Bestellungen von Kunden an Ihre Angestelten in der GRÜNEN Zone weiterleiten soll. Mit einer traditionellen Firewallkonfiguration würde dies nicht gehen, weil die Anfrage, auf die GRÜNE Zone zuzugreifen von außerhalb der GRÜNEN Zone initiiert wurde. Sie möchten sicherlich nicht allen Ihren Kunden direkten Zugriff auf die Rechner auf der GRÜNEN Seite gewähren. Wie kann eine solche Anforderung nun erfüllt werden? Durch die Einrichtung einer DMZ und die Benutzung von DMZ-Schlupflöchern.

DMZ-Schlupflöcher geben Rechnern in der ORANGEN Zone (DMZ) begrenzten Zugriff auf bestimmte Ports auf Rechnern in der GRÜNEN Zone. Da Server (die Rechner in der ORANGEN Zone) gelockerte Regeln hinsichtlich der ROTEN Zone haben, sind sie anfälliger für Hacker-Angriffe. Dadurch daß von ORANGE nach GRÜN nur ein beschränkter Zugriff zugelassen wird, werden unberechtigte Zugriffe auf geheime Bereiche verhindert, sollte der Server kompromittiert werden.

Die TCP/UDP DropDown-Liste ermöglicht die Auswahl des Protokoll für die Regel. Größtenteils benutzen die Server TCP. Einige Spieleserver und Chatserver benutzen UDP. Wenn das Protokoll in der Serverdokumentation nicht beschrieben ist, wird in aller Regel TCP eingesetzt. Benutzten Sie das Protokoll, das auf der Seite zur Port-Weiterleitung festgelegt wurde.

Quell-Netz ist ein DropDown-Liste, welche die verfügbaren Quell-Netzwerke auf dem IPCop Server zeigt.

Quell-Netz ist die IP-Adresse des Rechners, dem Sie die Erlaubnis zum Zugriff auf ihre internen Server erteilen wollen.

Ziel-Netz ist eine DropDown-Liste, welche die verfügbaren Ziel-Netzwerke auf dem IPCop Server zeigt.

Ziel-Port ist der Port auf dem Rechner, welcher auf die Anfrage hört

Ziel-Netz ist die IP-Adresse des Rechner in der GRÜNEN oder BLAUEN Zone, der die Anfrage entgegennimmt.

Nachdem alle Informationen eingetragen sind, setzen Sie das Häkchen in das Aktiviert-Symbol und betätigen den Schalter Hinzufügen. Danach wird die Regel in den nächsten Abschnitt verschoben und dort als aktive Regel aufgelistet.

Der Abschnitt Aktuelle Regeln enthält alle Regeln, die momentan in Kraft sind. Um eine zu löschen, müssen Sie das # Papierkorb-Symbol anklicken. Um eine Regel zu bearbeiten, klicken sie auf das gelbe Bleistift-Symbol.

Zum de-/aktivieren einer Regel müssen Sie das Aktiviert-Symbol (das Häkchen links in der #Aktion-Spalte) der jeweiligen Adresse anklicken. Das Häkchen im Symbol verschwindet, wenn eine Regel deaktiviert ist. Um sie wieder zu aktivieren, müssen Sie das leere Kästchen erneut anklicken.

2.6.6. Zugriff auf BLAU

Auf dieser Administrationsseite können Sie Einstellungen für Wireless Accesspoints im BLAUEN Netzwerk, die sich mit dem IPCop Server verbinden dürfen, vorgenehmen. Die Nutzung dieses Features ist freigestellt. Sie können ohne Bedenken diesen Abschnitt übergehen, wenn Sie davon keinen Gebrauch machen wollen.

Anmerkung

Diese Seite wird nur angezeigt, wenn eine BLAUE Netzwerkkarte installiert und konfiguriert wurde.

Um eine Zugriff auf BLAU einzurichten gehen Sie wie folgt vor:

1. Benutzen Sie eine unterstützte Ethernetkarte um eine BLAUE Schnittstelle einzurichten.
2. Verbinden Sie einen Accesspoint mit dieser Ethernetkarte. (Benutzen Sie am Accesspoint den LAN Ethernet Port, wenn Sie die Auswahl unter mehreren Ports haben.)
3. Sie können DHCP benutzen, um dynamische oder statische IP-Adressen auf BLAU zu vergeben, wenngleich statische IP-Adressen wegen der Sicherheit der MAC-Adressen vorzuziehen sind. Für weitere Informationen zur Konfiguration von statischen Adressvergabezeiten wird auf den Abschnitt DHCP Server verwiesen.

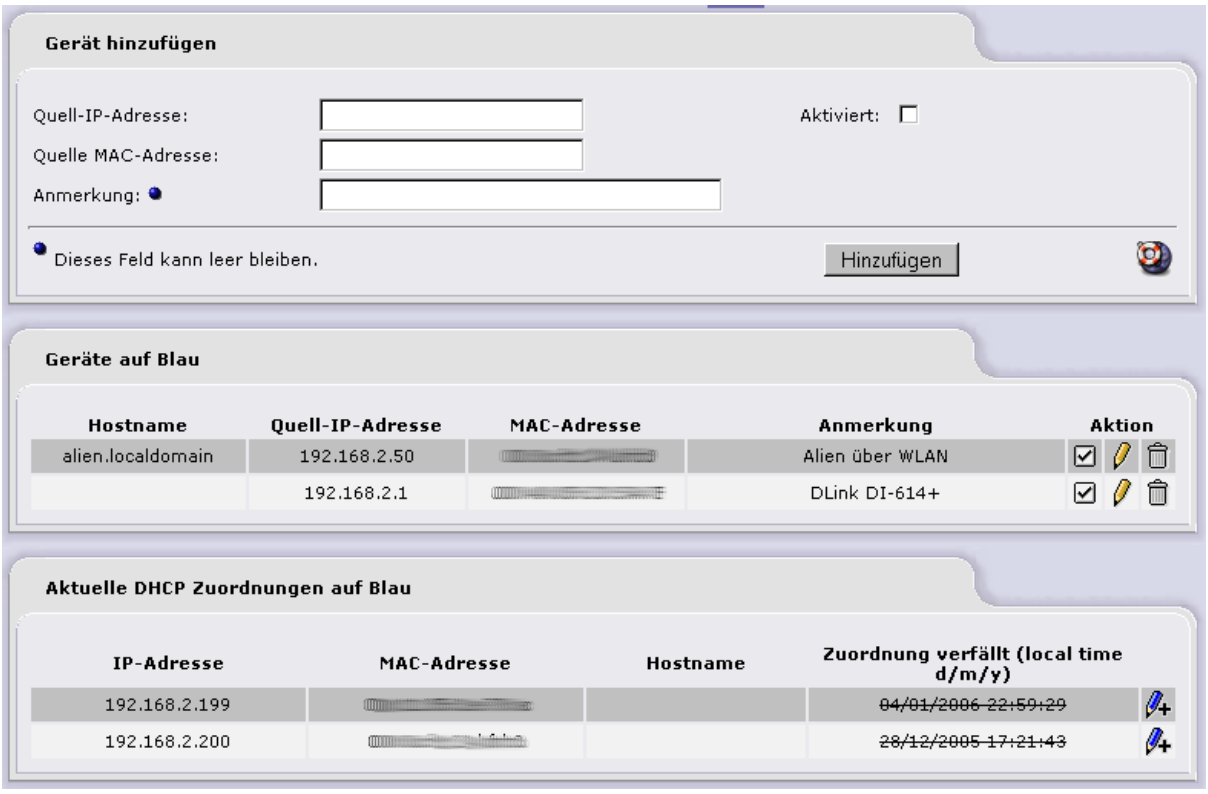
Wenn Sie auf dem BLAUEN Netzwerk nur http-Datenverkehr zum Internet (ROTES Netzwerk) bereitstellen müssen, tragen Sie die IP-Adress oder die MAC-Adress des Wireless Routers bzw. die einzelnen Wireless verbundenen Geräte, falls Sie einen Accesspoint benutzen, auf der Administrationsseite ein.

Ein Accesspoint verhält sich wie ein Ethernet Hub. IPCop vergibt DHCP-Leases durch ihn hindurch an die Wireless Geräte. Ein Wireless Router macht NAT, vergibt IP-Adressen an sein eigenes Subnetz per DHCP und hat seine eigene Zugangskontrollen.

Sie können das IPCop Webinterface von einem Computer im BLAUEN Netzwerk anzeigen. Sie können jedoch nicht zum GRÜNEN Netzwerk verbinden ohne einige zusätzlichen Handgriffe.

Um sich vom BLAUEN Netzwerk zum GRÜNEN Netzwerk zu verbinden, müssen Sie entweder:

1. die Seite DMZ-Schlupflöcher benutzen und für ihren Dienst entsprechende Schlupflöcher für BLAU einrichten
2. Ein VPN für Ihre RoadWarrior auf BLAU einrichten, um den Zugang bereitzustellen



Im Abschnitt Gerät hinzufügen tragen Sie die IP-Adresse oder die MAC Adresse eines Wireless Accesspoints oder jedes Geräts auf dem BLAUEN Netzwerk ein, welches über den IPCop Server zum Internet verbinden können soll.

Nachdem alle Informationen eingetragen sind, setzen Sie das Häkchen in das Aktiviert-Symbol und betätigen den Schalter Hinzufügen. Danach wird der Eintrag in den nächsten Abschnitt verschoben und dort als aktives Gerät aufgelistet.

Der Abschnitt Geräte auf Blau enthält alle aktuellen Einträge. Um eines zu löschen, müssen Sie das Papierkorb-Symbol anklicken. Um eines zu bearbeiten, klicken sie auf das gelbe Blestift-Symbol.

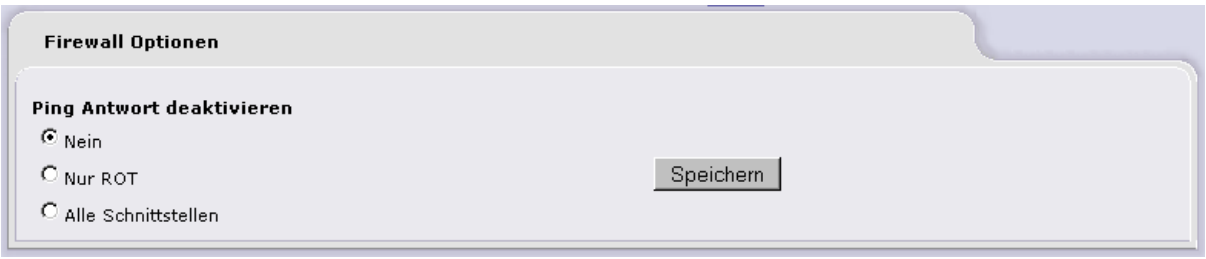
Zum de-/aktivieren eine Gerätes müssen Sie das Aktiviert-Symbol (das Häkchen links in der Aktion-Spalte) des jeweiligen Eintrages anklicken. Das Häkchen im Symbol verschwindet, wenn ein Gerät deaktiviert ist. Um es wieder zu aktivieren, müssen Sie das leere Kästchen erneut anklicken.

Wenn DHCP für das BLAUE Netzwerk aktiviert ist, wird der Abschnitt Aktuelle DHCP Zuordnungen auf Blau angezeigt.

Dort erhalten Sie ein schnelle Möglichkeit um Wireless Geräte zur Liste hinzuzufügen. Sie müssen lediglich auf das blaue Bleistift-Symbol klicken, um ein neues Gerät in die Liste der aktuellen Geräte aufzunehmen. Sie können dann den Eintrag, falls erforderlich, durch einen Klick auf das gelbe Bleistift-Symbolbearbeiten.

2.6.7. Firewall Optionen

Auf dieser Administrationsseite können Sie einige Einstellungen zum Verhalten der IPCop Firewall vornehmen. Die Nutzung dieses Features ist freigestellt. Sie können ohne Bedenken diesen Anschnitt übergehen, wenn Sie davon keinen Gebrauch machen wollen.



Ping Antwort deaktivieren

- Nein - IPCop Server beantwortet **ping**-Anfragen auf allen Schnittstellen. Dies ist das Standardverhalten.
- Nur ROT - IPCop Server beantwortet keine **ping**-Anfragen auf der ROTEN Schnittstelle.
- Alle Schnittstellen - IPCop Server beantwortet keine **ping**-Anfragen.

Um die Änderungen zu sichern, drücken Sie den Speichern.

2.7. VPNs

2.7.1. Virtual Private Networks (VPNs)

Virtual Private Networks oder VPNs erlauben es zwei Netzwerken sich direkt über ein anderes Netzwerk, z.B. das Internet, miteinander zu verbinden. Alle Daten werden sicher über einen verschlüsselten Tunnel versendet, geschützt vor neugierigen Augen. Auf die gleiche Weise kann sich ein einzelner Computer mit einem anderen Netzwerk verbinden. Eines der Protokolle die man braucht um ein VPN aufzubauen ist bekannt als IPSec.

IPCop kann sehr einfach VPNs zwischen anderen IPCop-Servern aufbauen. IPCop kann ebenfalls mit nahezu jedem VPN-Produkt welches IPSec und Standardverschlüsselungen wie z.B. 3DES zusammenarbeiten. Im IPCop werden VPN-Verbindungen als Netz-zu-Netz oder Host-zu-Netz definiert. Diese sind zu 100% optional; Sie sollten diesen Abschnitt also sicherhaltshalber ignorieren, wenn Sie diese Funktion nicht benutzen wollen.

Die meisten aktuellen Betriebssysteme unterstützen IPSec. Das beinhaltet Windows, Macintosh OSX, Linux und die meisten Unix-Varianten. Unglülicherweise bieten diese Tools sehr unterschiedliche Unterstützungen und könnten daher schwierig einzustellen sein.

2.7.1.1. Netz-zu-Netz

Netz-zu-Netz VPNs verbinden zwei oder mehr private Netzwerke über das Internet miteinander, indem sie einen IPSec- #Tunnel# aufbauen. In einem Netz-zu-Netz VPN muß mindestens eines der beteiligten Netzwerke per IPCop-Firewall mit dem Internet verbunden sein. Das andere Netzwerk kann an eine IPCop-Firewall angeschlossen sein, oder an einen anderen IPSec-fähigen Router oder Firewall. Diesen Routern/Firewalls wurde eine öffentliche IP von einem Provider zugewiesen und sie benutzen höchstwahrscheinlich NAT (Network Address Translation). Man nennt diese Konstellation daher Netz-zu-Netz.

Falls gewünscht kann auch ein VPN zwischen den wireless-Clients im BLAU-Netzwerk und der IPCop-Firewall aufgebaut werden. Das stellt sicher, dass der Datenverkehr im BLAU-Netzwerk nicht mit wireless-Sniffern abgehorcht werden kann.

2.7.1.2. Host-zu-Netz

Eine Host-zu-Netz Verbindung besteht, wenn der IPCop an dem einem Ende des VPN-Tunnels steht und ein Remote- oder Mobilbenutzer am anderen Ende. Der Mobilbenutzer ist höchstwahrscheinlich ein Laptop-Benutzer mit einer vom Provider zugewiesenen, dynamischen öffentlichen IP. Man nennt diese Konstellation daher Host-zu-Netz oder Roadwarrior.

2.7.2. Authentifizierungsmethoden

Bevor Sie eine Roadwarrior oder Netz-zu-Netz VPN-Verbindung konfigurieren können, müssen Sie sich für eine der Authentifizierungsmethoden pre-shared key (PSK) bzw. Passwort/Passphrase oder X.509-Zertifikat entscheiden. Mit der Authentifzierungsmethode identifiziert sich der Benutzer für den Zugang zum VPN.

2.7.2.1. Pre-shared Key

Die pre-shared key (PSK) Authentifizierungsmethode ist eine einfache Methode, die eine schnelle Konfiguration von VPNs ermöglicht. Für diese Methode geben Sie eine Authentifizierungsphrase ein. Dabei kann es sich um eine beliebige Zeichenfolge handeln, vergleichbar zu einem Passwort. Diese Phrase muss für die Authentifizierung beim IPCop und dem VPN-Client verfügbar sein.

Die PSK-Methode benötigt weniger Schritte als bei einer Authentifzierung über Zertifikate. Sie kann verwendet werden, um Verbindungstests durchzuführen und Erfahrungen beim Aufbau einer VPN-Verbindung zu sammeln. Erfahrene Benutzer sollten direkt zum Kapitel Erzeugen der Zertifikate für den IPCop springen, um eine Roadwarrior oder Netz-zu-Netz VPN-Verbindung aufzusetzen.

Die PSK-Methode sollte nicht mit Roadwarrior-Verbindungen benutzt werden, da all Roadwarrior die selbe Phrase benutzen müssen.

Anmerkung

Die *System-Uhrzeiten* an jedem Ende des VPN-Tunnels sollten *aktuell* sein, bevor das VPN konfigiriert wird.

2.7.2.2. X.509 Zertifikate

X.509 Zeritifikate stellen einen sehr sicheren Weg für die Verbindung von VPN-Servern dar. Um X.509-Zertifikate zu implementieren, müssen Sie entweder die Zertifikate auf dem IPCop erzeugen oder durch eine andere Zeritifizierungsstelle in Ihrem Netzwerk ausstellen lassen.

X.509 Begriffe

X.509 Zertifikate auf dem IPCop und vielen anderen Implementierungen werden über OpenSSL verwaltet. SSL (Secure Socket Layer) hat seine eigenen Begriffsdefinitionen.

X.509 Zertifikate enthalten, abhängig vom Anwendungsfall, öffentliche und private Schlüssel, Passphrasen und Informationen über die zugehörige Funktionseinheit. Diese Zertifikate dienen dazu, von Zertifizierungsstellen (Certificate Authorities oder CA) validiert zu werden. Webbrowsern beinhalten die CAs von öffentlichen Zertifizierungsstellen. Ein Host-Zertifikat wird von der dazugehörigen CA validiert. In privaten Netzwerken oder einzelnen Hosts kann die CA auf einer lokalen Maschine liegen. Im Falle von IPCop ist dies der IPCop selbst.

Zertifizierungsanfragen sind Anfragen für X.509 Zertifikate, die von CAs signiert (digital unterschrieben) werden. Dabei entsteht aus der Anfrage das eigentliche Zertifikat, das dann zum Anforderer zurückgeschickt wird. Dieses Zertifikat ist dann der CA bekannt, da es durch sie ausgestellt wurde.

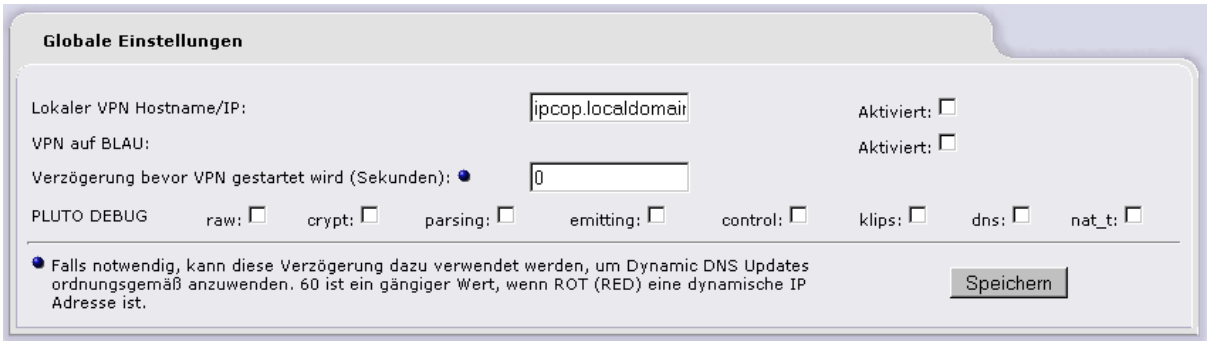
X.509 Zertifikate können in drei verschiedenen Formaten gespeichert werden, die Anhand der Datei-Endung erkannt werden können. PEM ist das Standard-Format für OpenSSL. Es kann alle zum Zertifikat gehörenden Informationen in lesbarer Form enthalten. Das DER-Format enthält nur die Key-Informationen und keine separaten X.509-Informationen. Dies ist das Standard-Format für die meisten Browser. Das PEM-Format ergänzt das DER-Format durch Kopf-Informationen. PKCS#12, PFK oder P12 Zertifikate enthalten im Binärformat die selben Informationen wie PEM-Dateien. Mit dem **openssl**-Kommando können die Formate untereinander konvertiert werden.

Um ein Zeritifikat benutzen zu können, muss es der Gegenstelle bekannt gemacht werden. Die IPSec-Implementierung von IPCop enthält ihre eigene, selbsterstellte CA. CAs können auch auf Roadwarrior-Maschinen laufen.

Wenn die IPSec-Implementierung auf den Roadwarrior-Maschinen keine eigenen CA-Fähigkeiten besitzt, können Sie eine Zertifikatsanforderung (Request) erstellen, die dann von der CA des IPCop signiert wird. Das dar-

aus resultierende Zertifikat kann dann auf der Roadwarrior-Maschine importiert werden.

2.7.3. VPN Globale Einstellungen



Geben Sie die VPN-Server-Details ein. Entweder den vollen Domainnamen oder die öffentliche IP-Adresse von der ROT-Schnittstelle. Wenn Sie einen dynamischen DNS-Service benutzen, sollten Sie hier den dynamischen DNS-Namen benutzen.

VPNs und dynamisches DNS

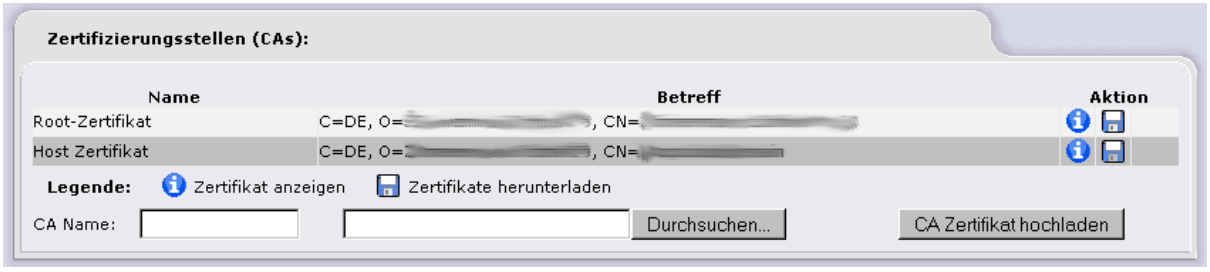
Falls Ihr Provider Ihre IP-Adresse geändert haben sollte (z.B. nach der Zwangstrennung) sind sie sich darüber bewusst, dass Sie die Netz-zu-Netz VPNs möglicherweise an beiden Enden des Tunnels neu starten müssen. Roadwarriors müssen in diesem Falle ebenfalls deren Verbindungen neu herstellen.

Aktivieren Sie VPN auf dem IPCop indem Sie lokaler VPN Hostname/IP ausfüllen, das Kästchen lokaler VPN Hostname/IP aktivieren und dann auf den Speichern-Knopf drücken. Die VPN auf BLAU Option ist nur dann sichtbar, wenn Sie vorher eine BLAU-Netzwerkkarte eingebunden und konfiguriert haben. Um ein VPN mit einer BLAU-wireless-Verbindung herstellen zu können, müssen Sie das Kästchen VPN auf BLAU-aktivieren.

2.7.4. Verbindungsstatus und -kontrolle

Um eine VPN-Verbindung zu erzeugen, benutzen Sie den Schalter Hinzufügen. Daraufhin erscheint die Seite für den VPN Verbindungstyp.

2.7.4.1. Erzeugen der Zertifikate für den IPCop



Um eine IPCop Zertifikats-Authority oder CA zu erstellen, geben Sie den Namen Ihrer CA in das entsprechende Textfeld ein. Der gewählte Name sollte sich vom Hostnamen des IPCop unterscheiden, um Mißverständnisse zu vermeiden. Zum Beispiel, ipcopca für die CA und ipcop für den Hostnamen. Dann klicken Sie auf den Schalter Root/Host Zertifikate erzeugen.

Die Seite zur Erstellung von Root/Host Zertifikaten erscheint. Füllen Sie das Formular aus und beide, ein X.509 Root und Host Zertifikat werden erzeugt.

Name der Organisation. Der Name der Organisation, den Sie im Zertifikat benutzen wollen. Wenn Ihr VPN zum Beispiel einige Schulen in einem Schulbezirk zusammenschließt, könnten Sie etwas wie **`Schulbezirk Ost`** als Namen verwenden.

Hostname des IPCop. Dies sollte der voll qualifizierte Domainname des IPCop sein. Wenn Sie einen dynamischen DNS nutzen, nehmen Sie diesen.

Ihre E-Mail Adresse. Ihre E-Mail Adresse, damit man mit Ihnen in Kontakt treten kann.

Die nächsten drei Angaben (Abteilung, Stadt und Staat/Bundesland) sind optional und können weggelassen werden.

Ihre Abteilung. Dies ist der Abteilungs- oder Unterabteilungsname. Um das Schulbeispiel weiterzuführen, könnte dies **`Offenburger Grund- und Hauptschulen`** sein.

Stadt. Die Stadt oder Postanschrift Ihrer Maschine.

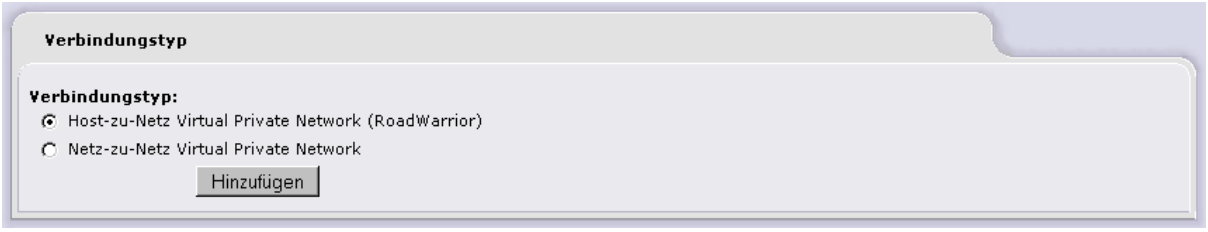
Staat oder Bundesland. Der Staat bzw. das Bundesland der Postanschrift.

Land. Dieses Pull-Down-Menü beinhaltet jeden bekannten ISO-Ländernamen. Benutzen Sie dieses zur Auswahl des Landes, das zum Zertifikat passt.

Nach dem vollständigen Ausfüllen des Formulars klicken Sie auf den Schalter Root/Host Zertifikate erzeugen, um die Zertifikate zu erzeugen.

Falls gewünscht, können mehrere Zertifikate auf einem IPCop erzeugt werden, welche dann in passwortgeschütze PKCS12-Dateien exportiert werden können. Sie können diese dann per E-Mail-Anhang an Ihre anderen Seiten schicken. Unter Benutzung der Funktion PKCS12 Datei hochladen dieser Seite können die Zertifikate auf einer lokalen IPCop-Maschine importiert und entschlüsselt werden.

2.7.4.2. Verbindungstyp



Wählen Sie entweder Host-zu-Netz (Roadwarrior) für mobile Anwender, die Zugriff zum grünen Netzwerk benötigen oder Netz-zu-Netz um Benutzern eines anderen Netzwerks Zugang zu Ihrem Grünen Netzwerk zu erlauben.

Wählen Sie den Verbindungstyp, den Sie erstellen möchten und klicken Sie auf den Schalter Hinzufügen.

Die nächste Seite die erscheint, beinhaltet zwei Bereiche. Der Verbindungs-Bereich kann je nach dem hinzuzufügenden Verbindungstyp variieren. Der Authentifizierungs-Bereich bleibt gleich.

2.7.4.2.1. Host-zu-Netz Verbindung

Name. Wählen Sie einen einfachen Namen (nur Kleinbuchstaben, ohne Leerzeichen) um diese Verbindung zu identifizieren.

Schnittstelle. Dann wählen Sie die Netzwerk-Schnittstelle, mit der sich der Roadwarrior verbinden soll (Rot oder Blau). Die Auswahl der Roten Schnittstelle erlaubt es dem Roadwarrior, sich vom Internet aus zu verbinden. Die Auswahl der Blauen Schnittstelle, erlaubt es dem Roadwarrior, sich über ein lokales WLAN mit dem Grünen Netzwerk zu verbinden.

Lokales Subnetz. Lokales Subnetz entspricht dem Grünen Netzwerk. Falls gewünscht, kann ein Subnetz des Grünen Netzwerks definiert werden, um den Zugang zum Grünen Netz für Roadwarrior einzuschränken.

Bemerkung. Bemerkung erlaubt es, eine optionale Bemerkung einzugeben, welche im VPN-Verbindungsfenster des IPCop für diese Verbindung erscheint.

Aktivieren. Klicken Sie das Kontrollkästchen an, wenn Sie diese Verbindung aktivieren wollen.

Bearbeiten der Einstellungen für Fortgeschrittene. Klicken Sie das Kontrollkästchen Bearbeiten der fortgeschrittenen Einstellungen nach Fertigstellung an, wenn Sie die Standardeinstellungen des IPCop für IPSec verändern wollen.

2.7.4.2.2. Netz-zu-Netz Verbindung

Name. Wählen Sie einen einfachen Namen (nur Kleinbuchstaben, ohne Leerzeichen) um diese Verbindung zu identifizieren.

IPCop Seite. Wählen Sie eine Seite für den IPCop, Rechts oder Links, die in den IPSec Konfigurationsdateien verwendet wird, um die Seite der Verbindung dieses IPCops auf dieser Maschine zu identifizieren. Hinweis: Die Seite bedeutet keinen Unterschied.

Lokales Subnetz. Lokales Subnetz entspricht dem Grünen Netzwerk. Falls gewünscht, kann ein Subnetz des Grünen Netzwerks definiert werden, um den Zugang zum Grünen Netz für Roadwarrior einzuschränken.

Entfernter Host/IP. Geben Sie hier die feste IP-Adresse des IPSec-Servers des entfernten Netzwerkes an. Sie können auch den kompletten, qualifizierten Domänennamen des entfernten Servers angeben. Wenn der entfernte Server einen dynamischen DNS-Dienst benutzt, könnte es sein, daß Sie das VPN neu starten müssen, falls sich die IP-Adresse ändert. Für diesen Vorgang gibt es in den IPCop Newsgroups diverse Skripts, die dies für Sie erledigen.

Entferntes Subnetz. Geben Sie die Netzwerk-Adresse und Subnetz-Maske des entfernten Netzwerks im selben Format wie das lokale Subnetz-Feld an. Dieses Netzwerk muß sich vom lokalen Subnetz unterscheiden, weil IPSec Routing-Tabellen-Einträge erstellt, um IP-Pakete zum richtigen entfernten Netzwerk zu schicken.

Bemerkung. Bemerkung erlaubt es, eine optionale Bemerkung einzugeben, welche im VPN-Verbindungsfenster des IPCop für diese Verbindung erscheint.

Aktivieren. Klicken Sie das Kontrollkästchen an, wenn Sie diese Verbindung aktivieren wollen.

Bearbeiten der Einstellungen für Fortgeschrittene. Klicken Sie das Kontrollkästchen Bearbeiten der fortgeschrittenen Einstellungen nach Fertigstellung an, wenn Sie die Standardeinstellungen des IPCop für IPSec verändern wollen.

Hinweise zur IPSec Terminologie

IPSec benutzt die Begriffe *Rechts* und *Links* für die beiden Seiten einer Verbindung bzw. eines Tunnels. Diese Begriffe haben keine wirkliche Bedeutung. IPSec orientiert sich anhand von Netzwerkadressen und Routen. Wenn es einmal festgestellt hat, welche Netzwerkverbindung (Rechts oder Links) zu benutzen ist, um auf die andere Seite der Verbindung zu gelangen, folgen alle anderen Rechts/Links Parameter automatisch. Viele benutzen Links für die lokale Seite einer Verbindung und Rechts für die entfernte Seite. Dies ist nicht notwendig. Es ist am Besten, wenn man sich das Ganze als „Seite A“ und „Seite B“ einer alten Langspielplatte vorstellt.

2.7.4.3. Authentifizierung

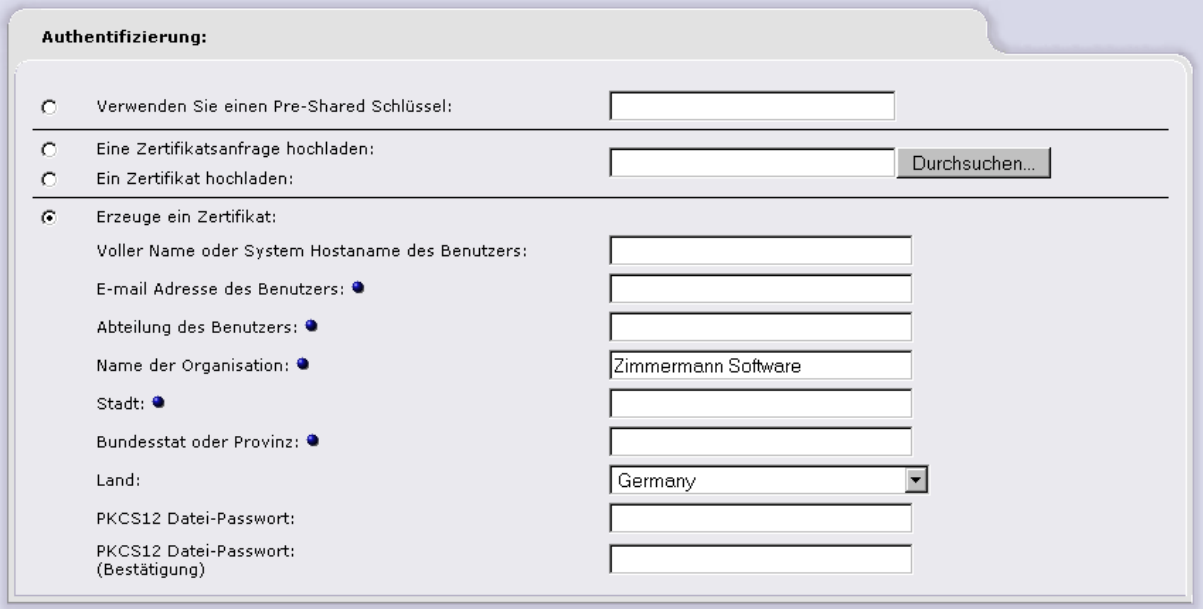
Der zweite Abschnitt der Seite beschäftigt sich mit der Authentifizierung. Anders ausgedrückt ist dies die Methode, wie der IPCop sicherstellt, daß der von beiden Seiten der Schnittstelle erstellte Tunnel mit der korrespondierenden Gegenstelle spricht. IPCop hat alle Anstrengungen unternommen, um PSKs und X.509 Zertifikate zu unterstützen. Es gibt vier gegenseitige exklusive Möglichkeiten, die für die Authentifizierung einer Verbindung benutzt werden können.

Benutzen eines Pre-Shared Keys. Geben Sie ein Passwort ein, um die Gegenseite des Tunnels zu authentifizieren. Wählen Sie diese Möglichkeit, wenn Sie ein einfaches Netz-zu-Netz VPN möchten. Sie können auch PSKs benutzen, wenn Sie damit experimentieren, ein VPN einzurichten. *Benutzen Sie keine PSKs um Tunnel zu Roadwarriorn zu authentifizieren.*

Zertifikats-Anfrage hochladen. Einige Roadwarrior IPSec Implementationen haben kein eigenes CA. Wenn sie das in IPSec implementierte CA benutzen wollen, können sie eine sogenannte Zertifikats-Anfrage erzeugen. Diese ist ein Teil des X.509 Zertifikats, welches vom CA signiert werden muß, um ein komplettes Zertifikat zu werden. Während des Zertifikats-Anfrage uploads wird die Anfrage signiert und das neue Zertifikat wird auf der Hauptseite des VPN verfügbar gemacht.

Zertifikat hochladen. In diesem Fall hat der Peer-IPSec ein CA zur Benutzung verfügbar. Beide, das CA-Zertifikat des Peers und das Host-Zertifikat müssen hochgeladen werden.

Erzeuge ein Zertifikat . In diesem Fall ist der IPSec-Peer in der Lage, ein X.509 Zertifikat vorzuweisen, hat aber nicht die Kapazität, um eine Zertifikats-Anfrage zu stellen. Füllen Sie für diesen Fall die benötigten Felder aus. Optionale Felder werden durch blaue Punkte gekennzeichnet. Wenn dieses Zertifikat für eine Netz-zu-Netz Verbindung sein soll, muß das Feld Benutzername oder das Hostnamens-Feld eventuell der volle qualifizierte Internet-Domainname des Peers sein. Der optionale Name der Organisation soll dazu dienen, verschiedene Teile einer Organisation vom Zugang zum kompletten Grünen Netzwerk des IPCop zu isolieren. Dies geschieht durch subnetting des lokalen Subnetzes im Verbindungsdefinitionsteil dieser Webseite. Die PKCS12-Datei Passwortfelder stellen sicher, daß die erzeugten Host-Zertifikate während der Übertragung zum IPSec-Peer nicht abgefangen oder kompromittiert werden können.



2.8. Logs

2.8.1. Einleitung

Die Administrationsseite "Logs" besteht entsprechend der gewählten Konfiguration von IPCop aus fünf oder aus sechs Unterseiten: # Logdatei-Einstellungen, Log Zusammenfassung, Proxy-Logdateien, Firewall-Logdateien, IDS-Logdateien (falls die Einbrucherkennung aktiviert ist) und System-Logdateien. Diese verfügen über in allen Unterseiten gleichermaßen vorhandene Steuerelemente, über die die anzuzeigenden Informationen ausgewählt und auf den lokalen Computer exportiert werden können. Über die Dropdownlisten Monat und Tag im Bereich Einstellungen der Administrationsseite können Sie die Protokollierungsinformationen für die vorangehenden Tage und Monate auswählen. Wenn Sie aus den Dropdownlisten Monat bzw. Tag neue Werte auswählen, müssen Sie auf die Schaltfläche Aktualisieren klicken, damit die angezeigten Protokolldaten aktualisiert werden. Wenn Sie eine Unterseite öffnen, werden zunächst die Protokolldaten für das aktuelle Datum angezeigt. Logdatei-Einstellungen, Log Zusammenfassung, Proxy-Logdateien, Firewall-Logdateien, IDS-Logdateien (falls die Einbrucherkennung aktiviert ist) und System-Logdateien. Diese verfügen über in allen Unterseiten gleichermaßen vorhandene Steuerelemente, über die die anzuzeigenden Informationen ausgewählt und auf den lokalen Computer exportiert werden können. Über die Dropdownlisten Monat und Tag im Bereich Einstellungen der Administrationsseite können Sie die Protokollierungsinformationen für die vorangehenden Tage und Monate auswählen. Wenn Sie aus den Dropdownlisten Monat bzw. Tag neue Werte auswählen, müssen Sie auf die Schaltfläche Aktualisieren klicken, damit die angezeigten Protokolldaten aktualisiert werden. Wenn Sie eine Unterseite öffnen, werden zunächst die Protokolldaten für das aktuelle Datum angezeigt.

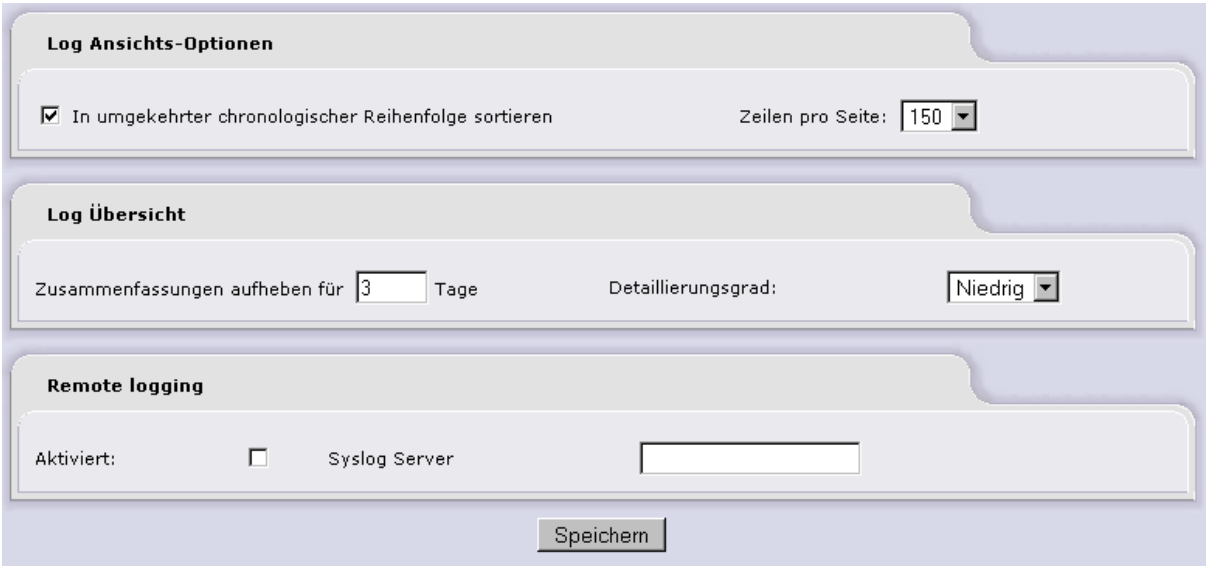
Mit den Schaltflächen << bzw. >> können Sie schnell einen Tag zurück bzw. vorwärts navigieren.

Die Protokollinformationen werden als Liste im Hauptabschnitt der Seite (die i. d. R. mit der Beschriftung Log versehen ist) angezeigt. Ist diese Liste so umfangreich, dass sie nicht mehr in einem normal großen Fenster angezeigt werden kann, werden nur die neuesten Protokollinformationen angezeigt. In diesem Fall werden oberhalb und unterhalb dieses Fensterausschnitts die zwei Links Älter und Neuer aktiviert, über die Sie durch die Protokolldaten blättern können.

Durch Klicken auf die Schaltfläche Exportieren wird eine Textdatei mit dem Namen `log.dat` mit den auf der aktuellen Logs-Administrationsseite enthaltenen Daten von dem IPCop-Server auf Ihren Computer heruntergeladen. In Abhängigkeit von der Konfiguration Ihres Computers wird durch Klicken auf die Schaltfläche Export ein Dialogfeld für den Dateidownload angezeigt, oder der Inhalt der Datei `log.dat` wird in einem Browserfenster oder als Textdatei im Standard-Text-Editor des Systems angezeigt. In den beiden letzten Fällen können Sie die Datei `log.dat` bei Bedarf als Textdatei speichern.

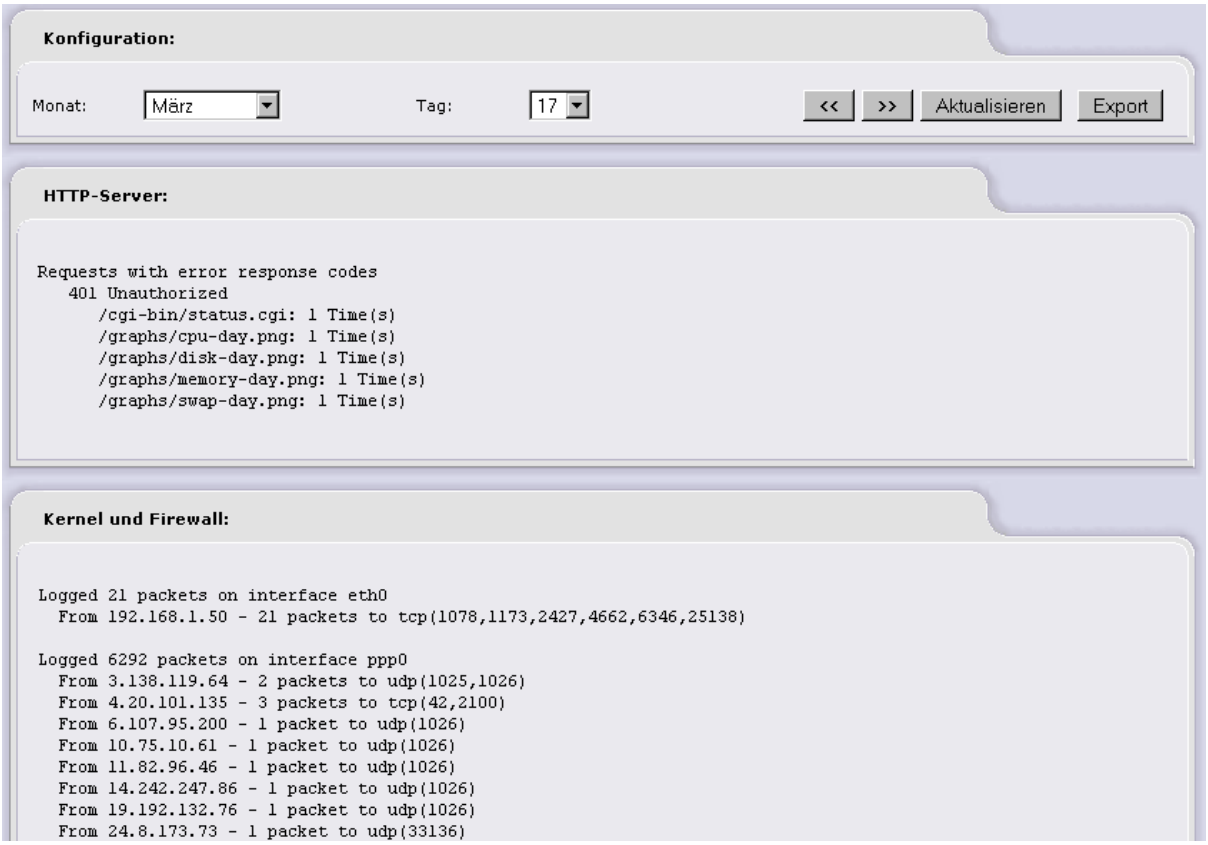
2.8.2. Logdatei-Einstellungen

Dokumentation wird ergänzt...



2.8.3. Log Zusammenfassung

Dokumentation wird ergänzt...



2.8.4. Proxy-Logdateien

Über diese Seite können Sie die Dateien anzeigen, die von der Webproxy-Komponente in IPCop zwischengespeichert worden sind. Nach der Installation von IPCop ist der Webproxy zunächst deaktiviert, die Komponente kann jedoch über die zugehörige Administrationsseite (Dienste > Proxy) aktiviert und bei Bedarf wieder deakti-

viert werden.

Anmerkung

Der Menübefehl Proxy-Logdateien ist nur dann verfügbar, wenn Sie auf der Administrationsseite Dienste > Proxy die Protokollierung aktiviert haben.

Aufgrund der umfangreichen Datenmengen, die beim Aufruf dieser Seite verarbeitet werden müssen, kann die Anzeige der Seite Proxy-Logdateien nach dem Aufruf oder einer Aktualisierung der Anzeige eine recht lange Zeit in Anspruch nehmen.

Neben den bereits zu Beginn des Abschnitts beschriebenen Steuerelementen Monat, Tag und Aktualisieren sind die folgenden Steuerelemente verfügbar:

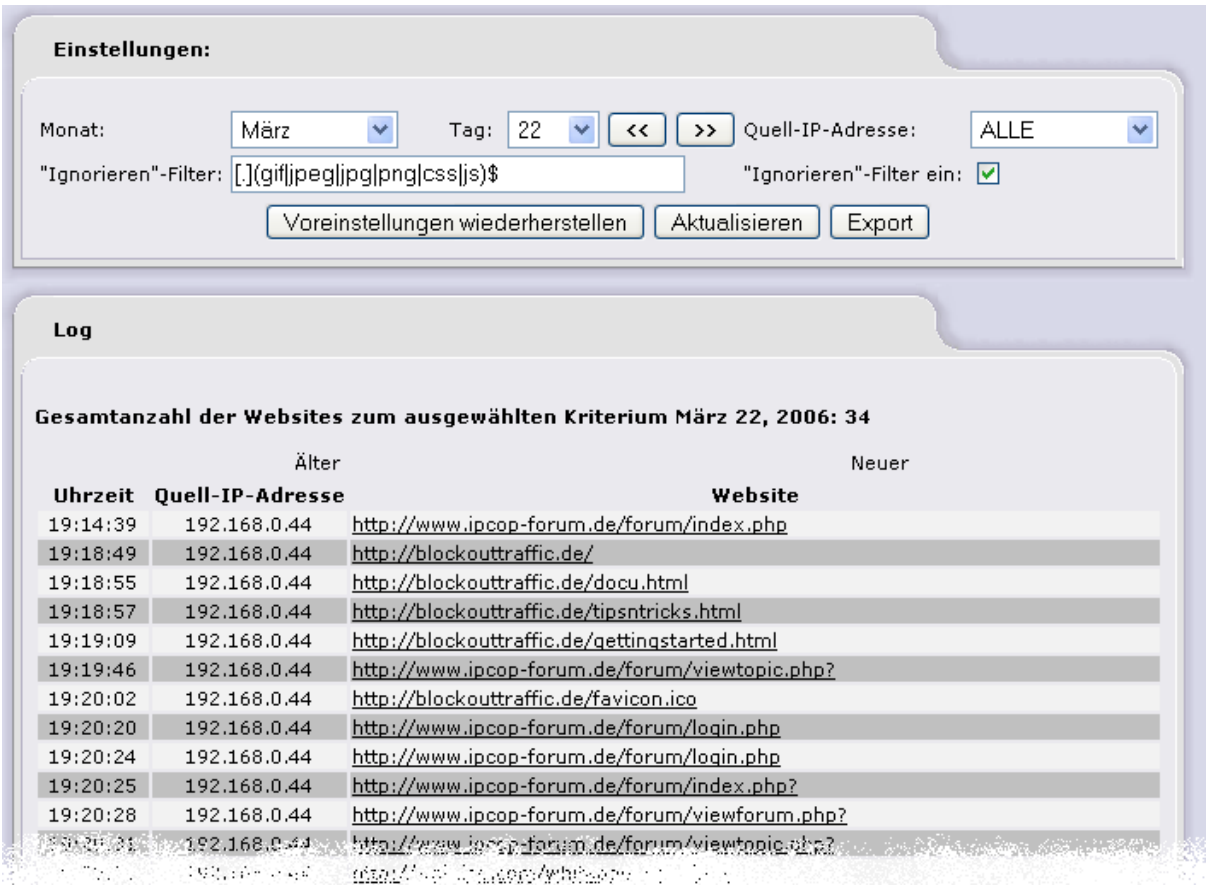
- Über die Dropdownliste Quell-IP-Adresse können Sie die Anzeige der Aktivitäten in Zusammenhang mit dem Web-Proxy auf einzelne IP-Adressen im lokalen Netzwerk einschränken. Alternativ können Sie auch die Aktivitäten für ALLE Computer, die den Proxy verwenden, anzeigen.
- Über das Feld Ignorieren-Filter können Sie reguläre Ausdrücke eingeben, mit denen festgelegt wird, welche Dateitypen von der Protokollierung des Webproxys ausgenommen werden sollen. Standardmäßig werden Grafikdateien (.gif, .jpeg, .png und .png), Stylesheet-Dateien (.css) und JavaScript-Dateien (.js) von der Anzeige ausgeschlossen.
- Mit dem Kontrollkästchen Ignorieren-Filter ein können Sie den über das Feld Ignorieren-Filter festgelegten Filter aktivieren bzw. deaktivieren.
- Klicken Sie auf die Schaltfläche Voreinstellungen wiederherstellen, um die genannten Steuerelemente und Filter auf die Standardeinstellungen zurückzusetzen.

Für diese Administrationsseite werden im Bereich Protokoll des Fensters die folgenden Informationen angezeigt:

- Die Uhrzeit, zu der die Datei angefordert und zwischengespeichert wurde.
- Die Quell-IP-Adresse des lokalen Computers, von dem die Anforderung stammt.
- Die Website (bzw. der URL) der angeforderten und zwischengespeicherten Datei.

Anmerkung

Die URL-Einträge von Websites in diesen Protokollen sind als Links zu den Webseiten bzw. Dateien implementiert, auf die verwiesen wird.



2.8.5. Firewall-Logdateien

Auf dieser Seite werden die Datenpakete angezeigt, die von der IPCop-Firewall gesperrt wurden.

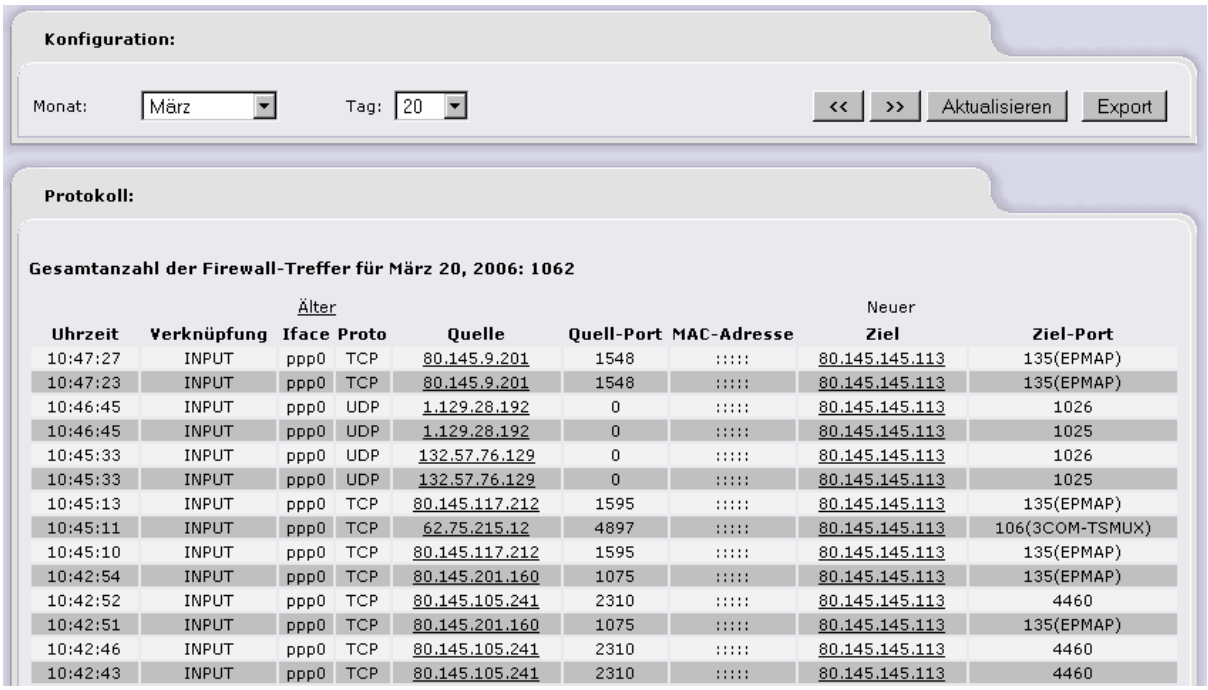
Anmerkung

Nicht alle zurückgewiesenen Datenpakete stellen Versuche mit bösartiger Absicht dar, Zugriff auf den Computer zu erhalten. Pakete können aus zahlreichen Gründen gesperrt werden, die keinen Anlass zur Beunruhigung geben sollten und daher einfach ignoriert werden können. Zu diesen gehören beispielsweise Verbindungsversuche zu dem „ident/auth“-Port (113), die von IPCop standardmäßig gesperrt werden.

Auf dieser Seite finden Sie die Dropdownlisten Monat und Tag, die Links << (vorheriger Tag) und >> (nächster Tag), sowie die Schaltflächen Aktualisieren und Export, die zu Beginn des Abschnitts beschrieben sind.

Im Bereich Protokoll der Seite wird für jedes der von der Firewall nicht angenommene Datenpaket jeweils ein Eintrag angezeigt. Der Eintrag besteht aus dem Zeitpunkt des Ereignisses, der Quell- und der Ziel-IP-Adresse für das zurückgewiesene Datenpaket, sowie das verwendete Protokoll, den Lauf durch IPCop und die verwendete Schnittstelle.

Sie können Informationen zu den angezeigten IP-Adressen abrufen, indem Sie auf die IP-Adresse klicken. IPCop ruft für die jeweilige IP-Adresse den zugehörigen DNS-Eintrag auf, und gibt einen Bericht mit den verfügbaren Informationen zur Registrierung und zum Eigentümer der IP-Adresse aus.



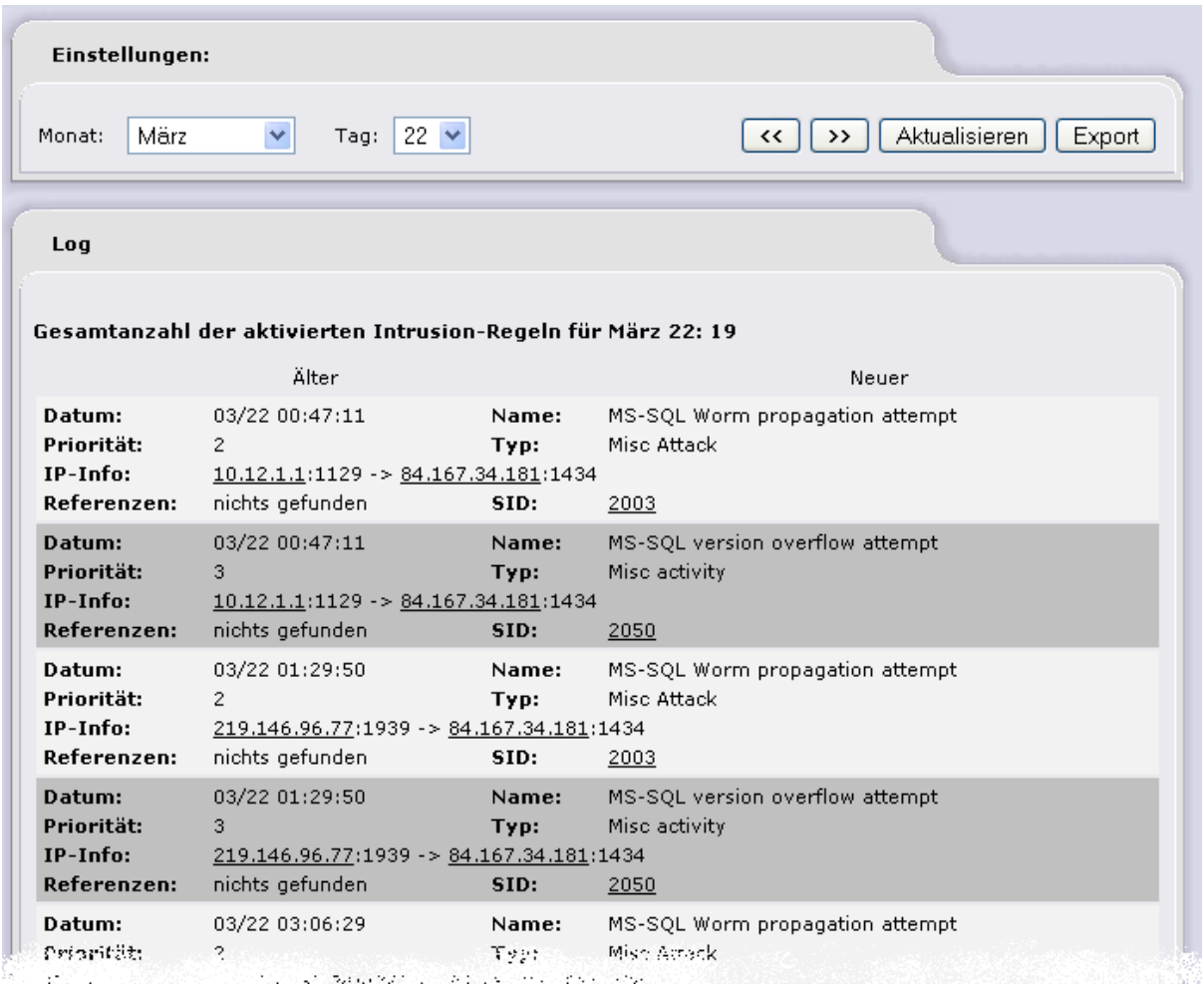
		Älter					Neuer	
Uhrzeit	Verknüpfung	Iface	Proto	Quelle	Quell-Port	MAC-Adresse	Ziel	Ziel-Port
10:47:27	INPUT	ppp0	TCP	80.145.9.201	1548	:::::	80.145.145.113	135(EPMAP)
10:47:23	INPUT	ppp0	TCP	80.145.9.201	1548	:::::	80.145.145.113	135(EPMAP)
10:46:45	INPUT	ppp0	UDP	1.129.28.192	0	:::::	80.145.145.113	1026
10:46:45	INPUT	ppp0	UDP	1.129.28.192	0	:::::	80.145.145.113	1025
10:45:33	INPUT	ppp0	UDP	132.57.76.129	0	:::::	80.145.145.113	1026
10:45:33	INPUT	ppp0	UDP	132.57.76.129	0	:::::	80.145.145.113	1025
10:45:13	INPUT	ppp0	TCP	80.145.117.212	1595	:::::	80.145.145.113	135(EPMAP)
10:45:11	INPUT	ppp0	TCP	62.75.215.12	4897	:::::	80.145.145.113	106(3COM-TSMUX)
10:45:10	INPUT	ppp0	TCP	80.145.117.212	1595	:::::	80.145.145.113	135(EPMAP)
10:42:54	INPUT	ppp0	TCP	80.145.201.160	1075	:::::	80.145.145.113	135(EPMAP)
10:42:52	INPUT	ppp0	TCP	80.145.105.241	2310	:::::	80.145.145.113	4460
10:42:51	INPUT	ppp0	TCP	80.145.201.160	1075	:::::	80.145.145.113	135(EPMAP)
10:42:46	INPUT	ppp0	TCP	80.145.105.241	2310	:::::	80.145.145.113	4460
10:42:43	INPUT	ppp0	TCP	80.145.105.241	2310	:::::	80.145.145.113	4460

2.8.6. IDS-Logdateien

Auf dieser Seite werden Ereignisse angezeigt, die von der IPCop-Einbruchsdetektierung (IDS) erkannt wurden. Nach der Installation von IPCop ist der die Einbruchdetektierung zunächst deaktiviert, die Komponente kann jedoch über die zugehörige Administrationsseite (Dienste > Einbruchdetektierung) aktiviert und bei Bedarf wieder deaktiviert werden.

Auf dieser Seite finden Sie die Dropdownlisten Monat und Tag, die Links << (vorheriger Tag) und >> (nächster Tag), sowie die Schaltflächen Aktualisieren und Export, die zu Beginn des Abschnitts beschrieben sind. Über diese Steuerelemente können Sie die IDS-Protokolle für einen bestimmten Tag anzeigen. Bei der Protokollierung werden eine Reihe von Merkmalen für den erkannten Einbruchversuch festgehalten:

- Das Datum und die Uhrzeit des Vorfalls.
- Name: - eine Beschreibung des Vorfalls.
- Priorität: (falls verfügbar). Die Priorität gibt den Schweregrad des Vorfalls an, in den Kategorien 1 (bösartig), 2 (nicht wirklich gefährlich) und 3 (möglicherweise schädlich).
- Art: - eine allgemeine Beschreibung des Vorfalls (falls verfügbar).
- IP Info: - die IP-Kennung (Adresse und Port) der beiden IP-Endpunkte (Ausgangs- und Zieladresse). Die IP-Adressen sind als Hyperlink implementiert, über den Sie den zugehörigen DNS-Eintrag aufrufen und einen Bericht mit den verfügbaren Informationen zur Registrierung und zum Eigentümer der IP-Adresse ausgeben können.
- Referenzen: - Hyperlinks zu URLs mit verfügbaren Informationsquellen zu dem jeweiligen Typ des Vorfalls.
- SID: - die Snort-ID (falls verfügbar). Bei „Snort“ handelt es sich um das von IPCop verwendete Softwaremodul für die IDS-Funktionalität; die SID ist der von dem Snort-Modul zur Kennzeichnung der verschiedenen Angriffsschemata verwendete ID-Code. Dieses Feld ist ebenfalls als Hyperlink zu einer Webseite mit dem zugehörigen Eintrag der Snort-Datenbank der Einbruchssignaturen implementiert.



2.8.7. System-Logdateien

Auf dieser Seite können Sie das Systemprotokoll sowie verschiedene weitere Protokolle anzeigen. (Informationen zur Verwendung der Dropdownlisten Monat und Tag, der Links << (vorheriger Tag) und >> (nächster Tag), sowie der Schaltflächen Aktualisieren und Export finden Sie am Anfang des Abschnitts.) Es sind elf verschiedene Protokollierungskategorien verfügbar, die über die Dropdownliste Abschnitt ausgewählt werden können:

- IPCop (Standardeinstellung) - allgemeine IPCop-Ereignisse wie das Speichern des PPP-Profils sowie Verbindungsinformationen (PPP has gone up on ppp0, „PPP wurde auf ppp0 gestartet“, oder PPP has gone down on ppp0, „PPP wurde auf ppp0 beendet“) für Einwählverbindungen.
- RED - Informationen zu dem Datenaufkommen für die IPCop-PPP-Schnittstelle. Hierzu gehören die Datenstrings, die an Modems und andere Netzwerkschnittstellen gesendet bzw. von diesen empfangen wurden. Diese Informationen können im Falle von Verbindungsproblemen zur Fehlerbehandlung herbeigezogen werden.
- DNS - zeigt das Protokoll von dnsmasq, dem Hilfsprogramm für den Domänennamensdienst, an.
- DHCP-Server - zeigt ein Protokoll der Aktivitäten der DHCP-Server-Funktionalität von IPCop an.
- SSH - stellt ein Protokoll der netzwerkbasierten Benutzeran- und -abmeldungen über die SSH-Schnittstelle bereit.
- NTP - zeigt ein Protokoll der Aktivitäten der ntpd-Server-Funktionalität an.
- Cron - stellt eine Aufzeichnung der Aktivitäten des cron-Dämons bereit.

- Login/Logout- stellt ein Protokoll der Benutzeran- und -abmeldungen am IPCop-Server bereit. Über diese Option werden sowohl lokale Anmeldungsvorgänge als auch solche, die über die SSH-Schnittstelle erfolgen, angezeigt.
- Kernel - Aufzeichnung der Kernel-Aktivitäten des IPCop-Servers.
- IPSec - Aufzeichnung der Aktivitäten von IPSec, dem von IPCop verwendeten VPN-Softwaremodul.
- Aktualisieren - Protokoll der Ergebnisse aller Updates, die für die IPCop-Software über das Fenster System > Updates installiert wurden.
- Snort - Protokoll der Aktivitäten des IDS-Systems.