

IPcop v1.3 und v1.4

Der Proxy-Server SQUID

<i>Inhaltsverzeichnis</i>	1
<i>Grundsätzliches</i>	1
<i>Vorbereitung</i>	1
<i>Beispiel eines Netzwerks</i>	2
<i>Was ist ein Proxy-Server?</i>	2
<i>Vorteile durch einen Proxy-Server</i>	3
<i>Squid und IPcop</i>	3
<i>Was also kann der Proxy-Server standardmässig auf dem IPcop?</i>	3
<i>Was kann er standardmässig nicht?</i>	3
<i>Warum schreibe ich dann über diese Funktionen?</i>	3
<i>Die Konfiguration</i>	4
<i>Übersicht</i>	4
<i>Erklärungen zu den einzelnen Optionen</i>	4
<i>Transparent contra Standard</i>	5
<i>Logfiles</i>	6
<i>Und jetzt?</i>	7

Grundsätzliches

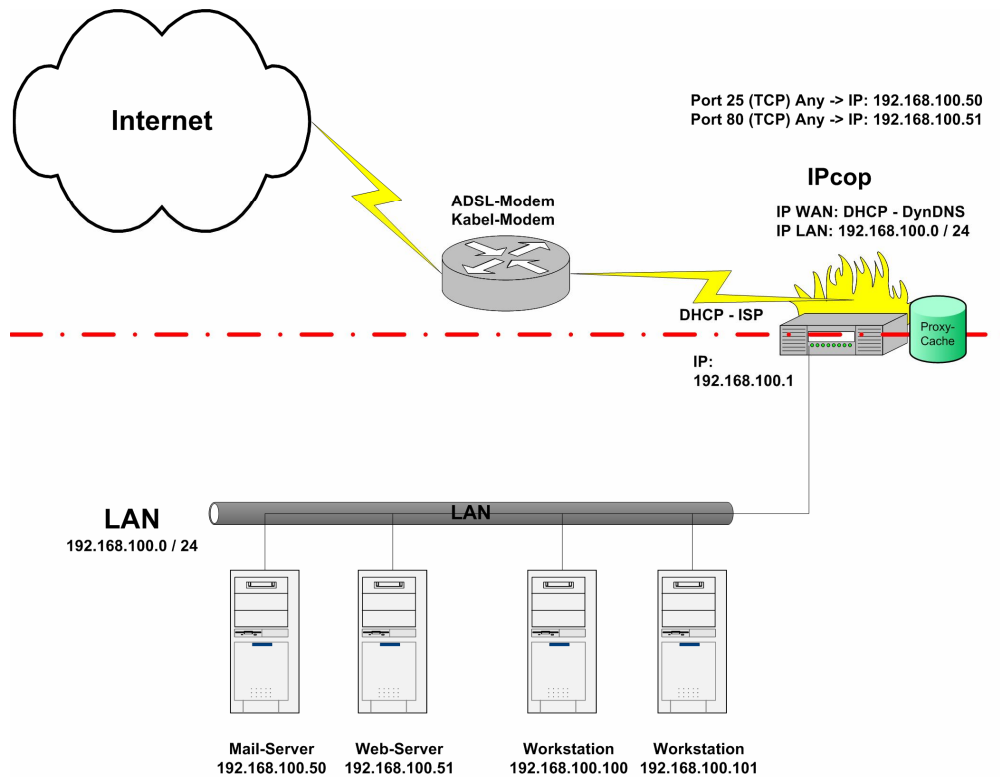
Dieses Tutorial setzt eine Grundkonfiguration wie in dem Tutorial zum Basissetup des IPcop voraus. Die IP-Adressen müssen gegebenenfalls an die lokalen Vorgaben angepasst werden.

Es werden die Einstellungen besprochen, die nötig sind, um den Proxy-Server des IPcop sinnvoll zu konfigurieren und zeigt einige praktische Einsatzmöglichkeiten auf.

Vorbereitung

1. Grundkonfiguration des IPcop nach einem der folgenden Tutorials:
http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_dyn.pdf
http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_fix.pdf
http://www.gutzeit.ch/ipcop/pdf/gr_konf_kabel_dyn_fix.pdf
2. Vorstellung, wie das Netzwerk aussehen soll

Beispiel eines Netzwerks



Was ist ein Proxy-Server?

Ein Proxy-Server hat im Netzwerk eine Vermittlungsfunktion. Er nimmt Anfragen von den Anwendern entgegen, lädt Daten aus dem Internet und leitet diese an den User weiter. Dabei können sowohl HTTP- als auch FTP-Inhalte über einen Proxy angefordert werden.

Der Server legt alle angeforderten Daten in einem Cache ab. Bevor der Proxy Daten aus dem Internet holt, wird überprüft, ob diese bereits im Cache vorliegen und noch aktuell sind. Ist dies der Fall, liefert der Server die Internet-Inhalte aus dem lokalen Speicher. Bei Daten, die häufig von verschiedenen Benutzern abgerufen werden, ergibt sich hieraus eine deutliche Reduzierung des Übertragungsvolumens. Zudem liefert der Cache die Inhalte häufig schneller, als wenn man diese aus dem Internet lädt.

Ein Proxy-Server kann prinzipiell vier verschiedene Funktionen, oder auch mehrere miteinander haben.

1. Caching, d. h. der Proxy-Server speichert alle Dateien, die er schon einmal heruntergeladen hat auf seiner lokalen Festplatte.
2. Security, d. h. da der Proxy-Server zum Internet hin als der anfragende Client erscheint, können gefährliche Antworten, Scripts, Viren, etc. schon auf dem Proxyserver abgefangen werden.
3. Filter, d. h. der Zugriff auf einzelne Seiten oder IPs kann gezielt blockiert werden.
4. Zugangsbeschränkung, d. h. wenn aktiviert, können nur authentifizierte Benutzer den Proxy-Server und damit das Internet nutzen.

Vorteile durch einen Proxy-Server

1. Caching beschleunigt den Zugriff auf Webinhalte und verringert das Transfervolumen.
2. Durch die Möglichkeit, z. B. Virens Scanner oder Spamfilter einzubinden, können Gefahren und andere Ärgernisse vom Endbenutzer ferngehalten werden.
3. Filter ermöglichen es dem Admin, bestimmte Domänen, IP-Ranges, oder auch Wörter/Wortbestandteile vom Zugriff auszuschliessen. Wortfilter sind jedoch mit Bedacht zu wählen, da das Wort „sex“ dem User auch den Zugriff z. B. auf Seiten über „Essex“ verwehrt.
4. Logging ermöglicht es dem Proxy-Betreiber, sowohl die Performance, als auch die besuchten Seiten, heruntergeladenen Files, etc. zu überwachen. Da so das Surfverhalten einzelner User nachvollzogen werden kann, ist diese Funktion mit Bedacht einzusetzen. **!!! Im geschäftlichen Umfeld ist aus Datenschutzrechtlichen Gründen die Auswertung der Logfiles nicht erlaubt!!!** Im privaten Umfeld stellt die Überwachung aber eine geeignete erzieherische Massnahme dar, die den Sprösslingen verdeutlicht, dass ihre Spuren im Internet jederzeit verfolgt werden können...

Squid und IPcop

Damit keine falschen Hoffnungen aufkommen. Nicht alle der oben aufgeführten Funktionen sind standardmässig auch auf dem IPcop verfügbar. Für viele gibt es jedoch so genannte MODs (auf die ich hier nicht näher eingehen möchte), die diese Funktionalität auch über das Webfrontend zugänglich machen.

Was also kann der Proxy-Server standardmässig auf dem IPcop?

- Cachen
- Loggen
- Performance-Messungen/Statistiken

Was kann er standardmässig nicht?

- User-Authentifizierung
- Überprüfung des Netzwerkverkehrs auf Viren, etc.
- Filtern nach Wörtern, IPs, Domänen

Warum schreibe ich dann über diese Funktionen?

All diese Funktionen lassen sich relativ einfach entweder mit frei verfügbaren Addons/MODs, oder mit wenigen Zeilen in der richtigen Datei, nachrüsten. Im Moment beschränkt sich dieses Tutorial jedoch auf die Standardfunktionen des IPcop. Mögliche Erweiterungen des Proxy-Servers werden nach und nach in dieses, oder ein spezielles Squid-MODs Tutorial einfliessen.

Die Konfiguration

Übersicht

The screenshot shows the IP Cop 1.4.2 configuration interface. The top navigation bar includes 'DIENSTE' and 'PROXY'. The main content area is titled 'Web-Proxy:' and contains the following settings:

- Aktiviert auf Green:**
- Transparent auf Green:**
- Aktiviert auf Blue:**
- Transparent auf Blue:**
- Log aktiviert:**
- Cache Verwaltung:**
 - Cache-Größe (MB):**
 - Min. Objektgröße (kB):**
 - Max. Objektgröße (kB):**
- Transferbeschränkungen:**
 - Max. eingehende Größe (kB):**
 - Max. abgehende Größe (kB):**
- Vorgelagerter Proxy (hostname:port):**
- Proxy-Benutzername:**
- Proxy-Passwort:**
- Proxy-Port:**

Buttons:

• Dieses Feld kann leer bleiben.

Erklärungen zu den einzelnen Optionen

Aktiviert: Ist wohl klar;-)

Transparent: s. Transparent contra Standard

Remote-Proxy: Falls der Provider einen Proxy-Server vorschreibt, kann hier der FQDN eingetragen werden.

Proxy-Benutzername: Falls der Remote-Proxy eine Authentifizierung verlangt, kann hier der Benutzername eingetragen werden.

Proxy-Passwort: Falls der Remote-Proxy eine Authentifizierung verlangt, kann hier das Passwort eingetragen werden.

Cache-Größe (MB): Anzahl Megabyte, die dem Proxy-Server für seinen Cache zur Verfügung gestellt werden sollen. Richtet sich nach der Größe der Festplatte und der Prozessorgeschwindigkeit. Hier 2 GB bei 8 GB HDD und PII 350 Mhz. Ein zu grosser Cache mit einer langsamen Festplatte und langsamem Prozessor kann den Aufbau von Webseiten auch verlangsamen!

Min. Objektgröße: Minimale Größe einer Datei, die im Proxy-Cache abgelegt werden soll. Kann auf 0 belassen werden.

Max. Objektgröße: Maximale Größe einer Datei, die im Proxy-Cache abgelegt werden soll. Hier 272 MB, so dass auch ein ganzes Windows-Servicepack Platz im Cache findet.

Max. eingehende Größe:

Hier kann die maximale Größe einer Datei festgelegt werden, die noch heruntergeladen werden darf. Wenn dieser Wert zum Beispiel auf „4096“ eingestellt würde, könnten maximal 4 MB grosse Dateien heruntergeladen werden. Dateien grösser als dieser Wert würden blockiert.

Max. abgehende
Grösse:

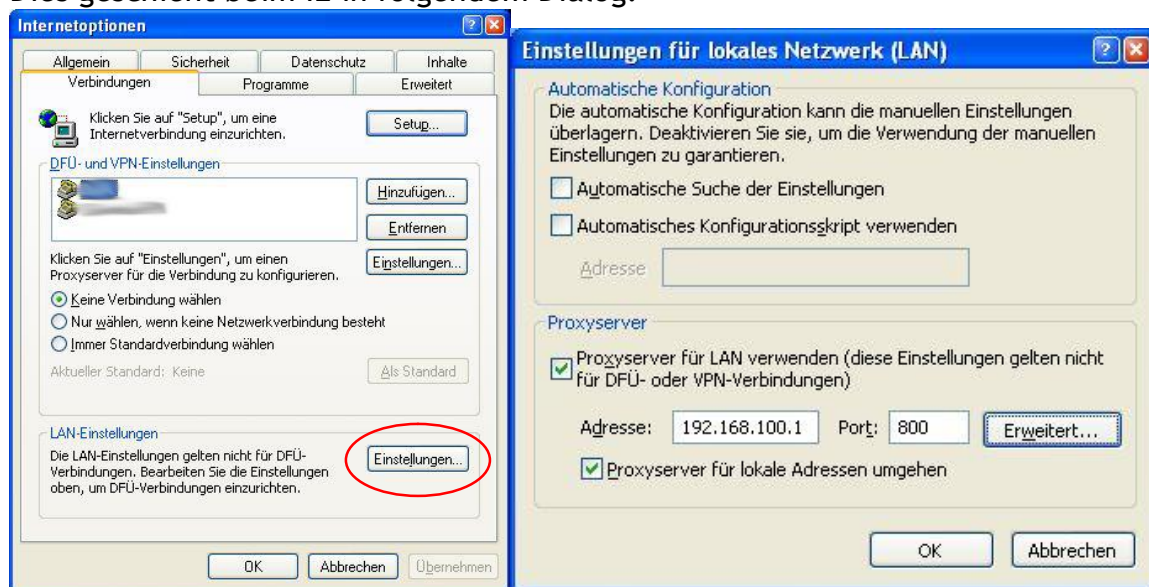
Hier kann die maximale Grösse einer Datei festgelegt werden,
die noch hochgeladen werden darf, s. o.

V1.4

Bei der v1.4 lässt sich zusätzlich der Proxy für das blaue Interface aktivieren, falls ein solches vorhanden ist.

Transparent contra Standard

Ein normaler Proxy-Server muss, damit er verwendet wird, zwangsweise in den Optionen des Browsers konfiguriert werden. Der Proxy-Port beim IPcop ist 800. Dies geschieht beim IE in folgendem Dialog:



Die Nutzung des Proxys lässt sich beim IPcop so aber leicht aushebeln, da das Entfernen des Häkchens bei „Proxyserver für LAN verwenden...“ dazu führt, dass die Anfragen nun direkt zum Webserver gesendet werden und der Proxy damit umgangen wird.

Beim transparenten Proxy-Server wird jede Anfrage auf den Ziel-Port 80 (HTTP) durch eine Firewall-Regel zum Proxy-Port 800 auf dem IPcop umgeleitet. Dadurch entfällt erstens die manuelle Konfiguration des Clients, da dieser wie gewohnt seine Anfrage an den Port 80 stellt, und zweitens ist eine Umgehung des Proxy-Servers durch diesen Automatismus auf dem Defaultgateway nun nicht mehr möglich, ohne den IPcop umzukonfigurieren.

fcki's Place

Für alle, die sich für die dazugehörige Firewall-Regel interessieren:

```
Chain SQUID (1 references)
pkts bytes target prot opt in out source destination
2508 120 REDIRECT tcp -- eth0 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 redir ports 800
```

Da die Konfiguration mit der Auswahl von „Transparent“ vollständig abgeschlossen ist (keine Änderungen auf dem Client nötig), ist dieser Ansatz zu bevorzugen.

Logfiles

Hier können alle Webseitenbesuche nachvollzogen werden, wenn gewünscht auch aufgeschlüsselt nach IP-Adresse (Wie ein PC, trotz DHCP, immer die gleiche IP-Adresse bekommt, ist im Tutorial http://www.gutzeit.ch/ipcop/pdf/dhcp_lan.pdf nachzulesen). Ein Klick auf einen der Einträge bringt einen direkt auf die gewünschte Seite. Hier ein Auszug aus den Logfiles meiner Tochter;-)

The screenshot shows the IPCop v1.3.0 web interface. The top navigation bar includes "Ansicht Proxy-Log", "System: IPCop", and "IPCOP v1.3.0". The main content area is titled "Konfiguration" and "Protokoll:". In the "Konfiguration" section, the "Quell-IP-Adresse" dropdown menu is set to "192.168.1.102". Below this, there is a filter input field containing "[.](gif|jpeg|jpg|png|css|js)\$" and a checkbox for "Ignorieren"-Filter ein: which is checked. Buttons for "Voreinstellungen wiederherstellen", "Aktualisieren", and "Export" are visible. The "Protokoll:" section displays a table of website visits for April 04: 20. The table has columns for "Uhrzeit", "Quell-IP-Adresse", and "Website". The log shows multiple visits from 192.168.1.102 to various websites including time.lab1.de, yetisports.org, siber.com, yeti3.yetisports.org, and e-medien.com. The interface also features a sidebar with navigation links like "Startseite", "Information", "Einwahl", "Dienste", "VPNs", "Logs", "System", and "Spam Filter", along with a penguin logo and a "SOURCEFORGE net" logo.

Uhrzeit	Quell-IP-Adresse	Website
13:40:10	192.168.1.102	http://time.lab1.de/?
13:40:11	192.168.1.102	http://time.lab1.de/?
13:40:31	192.168.1.102	http://www.yetisports.org/playonline.html
13:40:31	192.168.1.102	http://www.yetisports.org/playonline.html
13:40:33	192.168.1.102	http://www.yetisports.org/
13:40:34	192.168.1.102	http://www.yetisports.org/
13:40:39	192.168.1.102	http://www.siber.com/roboform/version.txt?
13:40:53	192.168.1.102	http://yeti3.yetisports.org/yetisportsdreia/index.php
13:41:00	192.168.1.102	http://yeti3.yetisports.org/yetisportsdreia/sec/score.php
13:41:04	192.168.1.102	http://yeti3.yetisports.org/yetisportsdreia/yeti3snd.swf
13:41:11	192.168.1.102	http://yeti3.yetisports.org/yetisportsdreia/sec/score.php
13:47:50	192.168.1.102	http://yeti3.yetisports.org/yetisports2/index.php
13:47:53	192.168.1.102	http://yeti3.yetisports.org/yetisports2/sec/score.php
13:48:02	192.168.1.102	http://yeti3.yetisports.org/yetisports2/ysp2.mod
13:55:21	192.168.1.102	http://www.yetisports.org/yetisports1/index.php
13:55:22	192.168.1.102	http://www.yetisports.org/yetisports1/yetisports1t.swf
14:02:36	192.168.1.102	http://www.e-medien.com/
14:02:42	192.168.1.102	http://www.e-medien.com/emed.swf
14:04:33	192.168.1.102	http://www.e-medien.com/
14:04:33	192.168.1.102	http://www.e-medien.com/emed.swf

Und jetzt?

- Wie wäre es mit dem Einrichten eines Web- oder Mail-Servers?
- Was ist eine DMZ und wofür brauche ich sie?
- Wie bringe ich meinen Webserver in der DMZ zum Laufen?

Also weiter geht's mit dem nächsten Tutorial.