Package C3SURF - Zugangskontrolle
Version 2.2.2

für den FLI4L Version 3.2.x

Das C3SURF-Team

Idee und Entwicklung
Frank Saurbier
mailto: c3surf@arcor.de

Dokumentationsbeabeitung
Helmut Backhaus
mailto: helmut.backhaus@gmx.de

8. Juli 2009

Inhaltsverzeichnis

1 Dokumentation des Paketes 3csurf

1.1 OPT_C3SURF

1.1.1 Kurzbeschreibung des Opt's

Du definierst, welche Hosts oder komplette Netzwerke von C3SURF verwaltet werden. Diese sind nach einem Routerstart zunächst gesperrt. http Anfragen dieser Hosts oder Netzclients werden auf die C3SURF Anmeldeseite geleitet. Nach der Registrierung eines Benutzers auf der Anmeldeseite kann Dein Netz auf Zeit von ihm genutzt werden. Alles wird gelogged - Du kannst über das Web Admin-Interface von C3SURF alles steuern.

1.1.2 Hinweise zur Installation

- Wie gehabt:
  - opt_c3surf_<versionsinfo>.tar.gz in das fli4l Verzeichnis (Buildrechner) entpacken.
  - c3surf.txt den eigenen Bedürfnissen anpassen (alles dort beschreiben).
  - ggf. in Deine httpd.txt die Rechte 'c3surf:view,admin' hinzufügen.
  - Build erstellen.
- Migration zur Version 2.2.2 (von 2.2.1)
  - Pflege die neue Variablen. Sie sind in der config.txt so
  - "# + new 2.2.2 + begin ———————— delete this line" gekennzeichnet.
  - C3SURF_CONTROL_SQUID: optional zur Kontrolle von squid, da squid nicht den Konventionen entspricht ist es vorläufig.
  - Die Variablen zum Überschreiben der Quota-Defaults bei LOGINUSR_ACCOUNT sind jetzt optional
- Migration zur Version 2.2.1 (von 2.2.0)
  - Pflege die neuen Variablen. Sie sind in der config.txt so
  - "# + new 2.2.1 + begin ———————— delete this line" gekennzeichnet.
  - C3SURF_WORKON_TMP: Empfehlung für Festplattenschlaf 'yes' sonst 'no' auch bei FLASH Medien (s.u.).
  - C3SURF_SAVE_QUOTA: Empfehlung 'yes' (s.u.).
- Migration zur Version 2.2.0 (von 2.1.0)
  - Pflege die neue Variable C3SURF_CHECK_ARPïn der config nach (Empfehlung: 'yes', s.u.). Sie ist in der config.txt so
  - "# + new 2.2.0 + begin ———————— delete this line" gekennzeichnet.

- Migration zur Version 2.1.0 (von früheren Versionen)
  - Pflege die neuen Variablen nach. Sie sind in der config.txt so
  - "# + new 2.1.0 + begin ———————— delete this line" gekennzeichnet.
  - Die MAC-Blackliste (so Du eine gepflegt hast) musst Du manuell ins Verzeichnis "C3SURF_PERSISTENT_PATH" kopieren.
  - Das Format der c3surf_login.log wurde um eine Spalte erweitert. Am besten die alte log sichern und in C3SURF_LOG_PATH löschen.

1.2 Config Datei und die Parameter

OPT_C3SURF Standard-Einstellung: `OPT_C3SURF='no'`

Paket aktivieren oder deaktivieren

C3SURF_LOG_PATH Standard-Einstellung: `C3SURF_LOG_PATH='/var/log/c3surf'`

Definiert das Verzeichnis für log-Dateien von C3SURF. Du musst mit moderatem Wachstum rechnen. Im Einzelen ist die bei den noch folgenden Einträgen für die Log-Dateien genannt. Beim Herunterfahren solltest Du die Logdateien auf ein permanentes Medium sichern oder den Pfad gleich dorthin einstellen, wenn Du die Dateien nicht verlieren willst. Der Pfad muss dann auf dem permanenten Medium existieren.

Wichtig: *Die 'c3surf_mac.blacklist' liegt ab sofort (v2.1.0) nicht mehr im C3SURF_LOG_PATH (Seite 5), sondern im persistenten Verzeichnis C3SURF_PERSISTENT_PATH (Seite 6). Falls Du eine Blacklist gepflegt hast, musst Du diese ins Verzeichnis C3SURF_PERSISTENT_PATH (Seite 6) kopieren. Weiter unten legst Du fest, was gelogged werden soll.*

C3SURF_DOLOG_LOGIN Standard-Einstellung: `C3SURF_DOLOG_LOGIN='yes'`

Zeichne Login / Logout auf: c3surf_login.log (default: 'yes')

C3SURF_DOLOG_INVALID Standard-Einstellung: `C3SURF_DOLOG_INVALID='yes'`

Zeichne ungültige Logins auf: c3surf_invalid.log (default: 'yes'). Wenn die OPT_LOGINUSR='yes' (Seite 13) gewählt ist, kann eine fehlerhafte Anmeldung zur Zeit nicht aufgezeichnet werden.

C3SURF_DOLOG_PAGE Standard-Einstellung: `C3SURF_DOLOG_PAGE='no'`

Zeichne den Aufruf der html-Seite auf: c3surf_page.log (default: 'no'). Jeder Zugriff auf die Anmeldeseite wird gelogged. Das Page-Log wächst vermutlich am 2. schnellsten von allen Logs - nur für Neugierige, die regelmäßig nachsehen.

C3SURF_DOLOG_HTTPD Standard-Einstellung: `C3SURF_DOLOG_HTTPD='no'`

Zeichne alle mini_httpd Anfragen auf: c3surf_httpd.log (default: 'no').

Zusätzlich die Mini-httpd Logfunktion starten, aber hier ist Vorsicht geboten, richtig schnelles Wachstum bitte nur für Test oder Debug verwenden. Wenn eingeschaltet, empfiehlt es sich wirklich täglich die log-Datei zu prüfen oder anders: Für ganz Neugierige - heißt regelmäßig prüfen und löschen.

opt_cpmvrmlog: `http://extern.fli4l.de/fli4l_opt-db3/search.pl?pid=427`
kann zum regelmäßigen wegsichern benutzt werden. Damit danach wieder korrekt gelogged wird, muss der mini_httpd neu gestartet werden. Dazu gibt es das Script "/usr/local/bin/c3surf_kill_httpd.sh" (Config Beispiel siehe im Anhang). (Seite 21)

C3SURF_PERSISTENT_PATH Unbedingt anpassen, Empfehlung: '/data/c3surf'

Definiert das Verzeichnes, welches Daten aufnimmt, die nach dem Ausschalten oder nach einem Reboot erhalten bleiben sollen. Idealerweise liegt dies auf einer Festplatte oder CF-Karte ('/data/c3surf'). Wer seine Platte lieber den ganzen Tag ausgeschaltet haben will, der kann auch ein Verzeichnis in der RAM-Disk wählen und sollte dann entsprechend seiner Anforderungen das Verzeichnis sporadisch auf die Platte kopieren (opt_sarfile oder opt_cpmvrmlog), sonst sind die Daten nach einem Reboot weg. Bei einem Absturz oder Stromverlust würden die Daten bis zur letzten Sicherung fehlen.

Was wird hier gespeichert:

- **MAC-Blackliste:**

  'c3surf_mac.blacklist',wird bei Bedarf angelegt (siehe Admin Interface). Also wenn Du dort Einträge veranlasst. Die Sperrung für die Mac-Adresse wurde bewusst über eine eigene Datei gelöst und nicht in den Paketfilter implementiert, da es bei einer größeren Zahl von Einträgen sonst Probleme geben kann. Aber nicht vergessen: Geblockte MAC-Adressen halten Standardbenutzer vom Netz fern, was im normalen Anwendungsfall ausreicht, nicht jedoch die Profis. Ausserdem verhindert diese MAC-Blacklist nur die Anmeldung über C3SURF / loginusr, weil es eben nicht direkt in der Firewall abgelegt wird.

- **Benutzerdaten:**

  <userloginname>.data (z. B. 'frank.data'), diese Dateien enthalten Daten über die Benutzer, wie Vorname, Name und E-mail-Adresse, welche auch im Web-Interface angezeigt werden. Weiter werden diese Dateien für Statistiken und die Kontrolle der Quotas benötigt. Die Persistenz der Benutzerdaten hat zur Folge, dass die Daten aus der Konfigurationsdatei nur noch beim ersten Mal erzeugt werden. Das heißt: Ist für den Benutzer "frank" eine 'frank.data' beim Systemstart vorhanden, so werden die Einstellungen in der Config-Datei ignoriert.

  Mittels LOGINUSR_ACCOUNT_x_OVERWRITE='yes' (Seite 14) kann das überschreiben der entsprechenden Benutzerdaten erzwungen werden. Mittels LOGINUSR_DELETE_PERSISTENT_DATA='yes' (Seite 13), werden alle "*.data" Dateien beim Reboot gelöscht (gleiches Verhalten wie ein temporäres Verzeichnis).

C3SURF_WORKON_TMP Standard-Einstellung: `C3SURF_WORKON_TMP='no'`

Wer eine Festplatte im Router verbaut hat und den C3SURF_PERSISTENT_PATH (Seite 6) auf diese Festplatte eingestellt hat, der kann hier 'yes' eintragen. Dann werden die persistenten Daten beim Router Start von der Festplatte auf das Verzeichnis C3SURF_TMP_PATH kopiert und nur noch von dort gelesen. Die Festplatte wird dann von C3SURF nicht mehr geweckt. Nur wenn Daten durch den Admin in die persistenten Dateien zurück geschrieben werden.

Wichtig: *Persistente Daten sind:*

- *Benutzer-Accounts*
- *MAC-Blackliste*
- *System Lock Datei (Verhindern jeder Anmeldung)*

Für FLASH-Speicher kann hier 'no' stehen, da ja im normalen Betrieb von C3SURF nur gelesen wird. Schreibzugriffe verursacht nur der Admin.

C3SURF_QUOTA Standard-Einstellung: `C3SURF_QUOTA='no'`

Soll der Zugang limitiert werden, wird hier 'yes' eingetragen. So wird der Zugang für eine IP-Adresse für C3SURF_BLOCKTIME (Seite 8) Minuten nach Zeitablauf oder überschreitung des Anmeldezählers blockiert. Als Standardwert wurde 'yes' gewählt. Ein 'no' entspricht dem Verhalten der C3SURF Versionen vor der Version 2.1.0.

Wichtig: *Auch die individuellen -TIME, -BLOCKTIME und -COUNTER bei den Accounts zum LOGIN_USR werden durch diese Variable aktiviert ('yes') oder deaktiviert ('no').*

C3SURF_COUNTER Standard-Einstellung: `C3SURF_COUNTER='0'`

Gibt die Anzahl der möglichen Unterbrechungen innerhalb der Freiminuten an.

Wichtig: *Seit der Version 2.1.0 werden die Freiminuten nicht mehr nur nach dem Parkuhrprinzip verwaltet: Einmal angemeldet läuft die Zeit ohne Unterbrechungsmöglichkeit sondern es kann eine Anzahl von Unterbrechungen (Logout/Login) definiert werden. Wird hier z. B. '1' eingetragen, so kann man sich innerhalb der Freiminuten einmal abmelden und dann wieder anmelden, was 2 Anmeldungen in der Zeit entspricht. Bei der folgenden Anmeldung erhält man die von C3SURF_TIME (Seite 8) noch verbliebene Differenz von der Anmeldung davor.*

Ist zudem C3SURF_BLOCKTIME='0' (Seite 8) gewählt, so wird der c3SURF_COUNTER erst nach 0:00 Uhr des Folgetages zurückgesetzt.

Der Wert 0 entspricht dem Parkuhrprinzip und bildet das Verhalten von c3Surf vor der Version 2.1.0 ab. Mit '-1' wird diese Funktion abgeschaltet = beliebig viele Unterbrechungen der Freiminuten sind möglich.

Ist C3SURF_QUOTA='yes' (Seite 7), so wird nach der Überschreitung des Zählers die Sperre entsprechend C3SURF_BLOCKTIME (Seite 8) aktiviert.

C3SURF_TIME Standard-Einstellung: `C3SURF_TIME='60'`

Anzahl der Minuten, die eine Freischaltung gilt.

C3SURF_BLOCKTIME Standard-Einstellung: `C3SURF_BLOCKTIME='240'`

Anzahl der Minuten, die eine IP geblockt wird, wenn die Freiminuten abgelaufen sind oder wenn der Admin dies über das Web-Interface veranlasst. So kann ein Rechner für diese Zeit aus dem Netz ferngehalten werden und die Nutzung eingeschränkt werden. Damit bei Zeitablauf die Sperrung erfolgt, muss C3SURF_QUOTA='yes' (Seite 7) eingestellt sein.

Sonderfälle:
'0': es erfolgt eine Sperrung der Adresse, bzw. des Nutzers bis 00:00 Uhr des Folgetages. '-1': es erfolgt keine Sperrung.

Die Aufhebung der Sperre ist mit einem mittleren Fehler von einer Minute behaftet.

C3SURF_SAVE_QUOTA Standard-Einstellung: `C3SURF_SAVE_QUOTA='yes'`

Sichere die Quota-Werte beim Herunterfahren und lade sie beim Start des Routers. Damit werden bei einem normalen Reboot des Routers die temporären Dateien der Quota-Verwaltung nach C3SURF_PERSISTENT_PATH (Seite 6) geschrieben und beim Neustart von dort wieder in das temporäre Verzeichnis eingelesen. So bleiben die momentanen Verbrauchsdaten der Benutzer erhalten. Ein plötzlicher Stromausfall ist damit nicht abgedeckt.

Wichtig: *LOGINUSR_DELETE_PERSISTENT_DATA='no' (Seite 13), sollte eingestellt sein, weil diese Option sonst beim Neustart alle Benutzer-Accounts und die zugehörigen Quota-Daten löscht.*

C3SURF_CHECK_ARP Standard-Einstellung: `C3SURF_CHECK_ARP='yes'`

Prüfe im Countdown Modul, ob die IP eines Rechners aus der ARP Tabelle verschwunden ist. So kann ein abgeschalteter Rechner erkannt werden. Jedoch manchmal mit erheblichem Zeitversatz.

C3SURF_CONTROL_HOST_OR_NET_N `C3SURF_CONTROL_HOST_OR_NET_N='0'`

Wert: Ganze Zahl.
Wieviele und welche IP-Bereiche oder Hosts sollen von c3Surf kontrolliert werden. Dies betrifft die Weiterleitung in ein anderes Netz (FORWARD Chain).

C3SURF_CONTROL_HOST_OR_NET_x

```
C3SURF_CONTROL_HOST_OR_NET_x='Netzwerk OR Host OR IP-Adresse'
```

Kontrolliert alle Clients.

Hier kann zur Vereinfachung ein komplettes Netz angegeben werden, z. B. das WLAN. Dann müssen alle WLAN-Nutzer die Anmeldeseite benutzen. Es können auch eine Referenz auf einen Host (@Host) oder eine IP-Adresse angegeben werden. Wer oder was hier eingetragen ist, wird auf die Anmeldeseite umgeleitet und es gelten die weiter unten zu definierenden Sperrregeln.

Beispiel:

```
C3SURF_CONTROL_HOST_OR_NET_1='IP_NET_3'       # Das Netz angeben IP/MASK
C3SURF_CONTROL_HOST_OR_NET_2='@T8200'         # oder den Host @HOST
C3SURF_CONTROL_HOST_OR_NET_3='192.168.13.11'  # oder eine IP-Adresse

Das nächsten Beispiel ist vom Prinzip her gleich mit dem oben bereits
dargestellten (IP_NET_3). Wenn in der "base.txt" die IP-Adresse so gesetzt
wurde.

C3SURF_CONTROL_HOST_OR_NET_1='192.168.0.1/24' # kontrolliert alle Clients

Soll ein Rechner ausgenommen sein, so kannst Du entweder alle IP-Adressen
einzeln in die C3SURF.txt aufnehmen (also eine Liste aller 256 Adressen
erstellen, wobei Du die eine weglässt), oder Du verwendest die CIDR Notation
(wie oben), dann sind es IP-Gruppen und damit ist es weniger Schreibarbeit
(8 Zeilen, statt 255).
```

Das sieht dann so aus:

```
C3SURF_CONTROL_HOST_OR_NET_N='8'                # Die Anzahl der Hosts
                                                # oder Netze
C3SURF_CONTROL_HOST_OR_NET_1='192.168.0.0/31'   # 0-1
C3SURF_CONTROL_HOST_OR_NET_2='192.168.0.3'      # only 3 not 2
C3SURF_CONTROL_HOST_OR_NET_3='192.168.0.4/30'   # 4-7
C3SURF_CONTROL_HOST_OR_NET_4='192.168.0.8/29'   # 8-15
C3SURF_CONTROL_HOST_OR_NET_5='192.168.0.16/28'  # 16-31
C3SURF_CONTROL_HOST_OR_NET_6='192.168.0.32/27'  # 32-63
C3SURF_CONTROL_HOST_OR_NET_7='192.168.0.64/26'  # 64-127
C3SURF_CONTROL_HOST_OR_NET_8='192.168.0.128/25' # 128-255

Jetzt kann der Rechner mit der IP '192.168.0.2' ohne Anmeldung alles was
in der firewall des fli4l erlaubt ist.
```

C3SURF_CONTROL_PORT_N `C3SURF_CONTROL_PORT_N='0'`

Wert: Ganze Zahl.
Wieviele TCP-Ports des Routers sollen gesteuert werden?

Wieviele und welche explizit benannten Ports sollen von c3Surf kontrolliert werden? Betroffen sind die IP-Bereiche und die Hosts von oben "C3SURF_CONTROL_HOST_OR_NET_N" (Seite 8). c3Surf steuert diese Ports und gibt diese nach einer erfolgreichen Anmeldung frei, so dass die über diese Ports existierenden Services des Routers genutzt werden können (betrifft die INPUT-Chain).

C3SURF_CONTROL_PORT_x `C3SURF_CONTROL_PORT_x='port_nr'`

Angabe der Portnummer und der Zugriff auf die dahinter stehenden Dienste des Routers (fli4l) sind bis zur Anmeldung gesperrt. Nach erfolgter Anmeldung der Dienst dann für die Zeit der Freischaltung zur Verfügung gestellt.

Beispiele:

```
C3SURF_CONTROL_PORT_1='515' # z.B. lpdsrv (Drucker benutzbar, nach
Anmeldung)
C3SURF_CONTROL_PORT_2='21'  # z.B. ftp - (wohl gemerkt ftp auf dem router!
                            # gibts ja nicht ;-))

Weitere mögliche Portadressen:
21=ftp, 22=ssh, 5000=imonc, 5001=telmod,
8118=privoxy, 9050=tor, 3128=squid, 20000=mtgcapri
80=http(Admin) 515=lpdsrv

Aber entscheidend ist die eigene Konfiguration. Es gelten für alle Ports,
die nicht angegeben sind natürlich immer die Regeln aus der 'base.txt'.
Nach einer Anmeldung gelten im übrigen auch immer noch die Regeln aus der
'base.txt'. c3Surf ist diesen Regeln bis zur Anmeldung durch den Benutzer
nur vorgeschaltet. Es werden also nach der Anmeldung immer noch alle Regeln
beachtet. So kann man z. B. in der 'base.txt' den Zugriff von WLAN auf das
kabelgebundene Netz verbieten. Dieses Verbot gilt dann natürlich auch für
die über c3Surf im WLAN angemeldeten Benutzer.
```

C3SURF_BLOCK_PORT_N `C3SURF_BLOCK_PORT_N='0'`

Wert: Ganze Zahl.
Wieviele TCP-Ports des Routers sollen geblockt werden?

Hinweise:
Permanentes Blocken von Diensten für oben benannte Netze und Hosts "C3SURF_CONTROL_HOST_OR_NET_N" (Seite 8). Wieviele und welche explizit benannten Ports sollen von c3Surf permanent geblockt werden? Es gibt dann keinen Zugriff auf die dahinter stehenden Dienste des Routers (fli4l) für die Hosts und/oder Rechner der gesperrten Netze. Auch nach dem Anmelden nicht. Betrifft die INPUT-Chain. Eigentlich ist diese Funktion nicht notwendig, denn wer bestimmte Dienste dauerhaft sperren will, sollte dies besser in der 'base.txt' mit den dortigen Parametern zur INPUT Chain tun.

Warum:
Weil diese Regeln hier nicht mehr gelten, sobald man den Parameter OPT_C3SURF='no' (Seite 5) setzt. Wer also C3SURF entsorgt, muss zuvor die hier definierten Regeln in die 'base.txt' übertragen, wenn ihm die Dienstesperre für die oben benannten Hosts oder Netze weiter wichtig sind.

C3SURF_BLOCK_PORT_x `C3SURF_BLOCK_PORT_x='port_nr'`

Beispiele:

```
C3SURF_BLOCK_PORT_1='5000'          # z.B. imonc
C3SURF_BLOCK_PORT_2='5001'          # z.B. telmond
C3SURF_BLOCK_PORT_3='20000'         # z.B. mtgcapri (OPT_MTGCAPRI)
C3SURF_BLOCK_PORT_4='22'            # z.B. ssh
C3SURF_BLOCK_PORT_5='8118'          # z.B. privoxy (PROXY)
C3SURF_BLOCK_PORT_6='9050'          # z.B. tor (PROXY)
C3SURF_BLOCK_PORT_7='80'            # z.B. httpd Admin interface (HTTPD)
C3SURF_BLOCK_PORT_8='7437'          # z.B. caiviar (OPT_CAIVIAR)
```

C3SURF_HTTPD_PORT Standard-Einstellung: `C3SURF_HTTPD_PORT='8080'`

Auf welchem Port und welcher IP-Adresse soll der mini_httpd für die Benutzeranmeldung lauschen? http Anfragen von Rechnern werden auf diese Adresse und diesen Port umgeleitet. Port 8080 ist hier Default.

Wichtig: *Folgendes ist bei der Wahl der Portnummer zu beachten*

- *Es sollte nicht der Port aus dem httpd-Paket sein (normal ist das 80).*
- *Der httpd für den Web-Admin des fli4l bindet sich im Standard an alle lokalen IP's.*
- *benutze auch keine Portnummer, die bereits von einem anderen Dienst genutzt wird.*

Solltest Du versehentlich einen bereits verwendeten Port erwischt haben, versucht der fli4l diesen httpd immer wieder zu starten. Was der nicht will, weil der Port schon vom Admin-Interface oder einem anderen Dienst belegt ist. Das kannst Du nur auf der Konsole oder in einem eingeschalteten Log sehen. Merken tust Du es daran, dass C3SURF nicht funktionieren wird, und dass Dein fli4l hohe CPU-Belastung hat und furchtbar langsam zu laufen scheint.

C3SURF_HTTPD_LISTENIP Standard-Einstellung: `C3SURF_HTTPD_LISTENIP='Host OR IPAdresse'`

Gibt die angegebene lokale IP an, an die sich das Interface für die Anmeldung binden soll. Entweder IP-Adresse oder @hostname. Hierhin werden http Anfragen der Clients bei Bedarf (also wenn sie nicht angemeldet sind) umgeleitet. So kommen die Anwender dann schnell auf die Anmeldeseite.

Beispiele:

```
C3SURF_HTTPD_LISTENIP='@wifi-router'  # Angabe eines Hostnamens in der
                                      # fli4l-Weise.
C3SURF_HTTPD_LISTENIP='192.168.11.3'  # Angabe einer IP-Adresse
C3SURF_HTTPD_LISTENIP='IP_NET1_IPADDR'
                                      # Angabe einer IP-Adresse mittels
                                      # Variable
                                      #
                                      # Der http-Diesnt für C3SURF wird immer
                                      # an genau eine IP-Adresse gebunden.
```

1.2.1 Optionale Parameter OPT_C3SURF

C3SURF_CONTROL_SQUID Standard-Einstellung: `C3SURF_CONTROL_SQUID='no'`

Optional:C3SURF_CONTROL_SQUID
Mit dem Einfügen der Variable C3SURF_CONTROL_SQUID='yes' wird die Kontrolle über squid erzwungen. Damit wird die C3SURF Portumleitung an den Anfang gesetzt, was auch Auswirkungen auf andere Pakete hat (z. B. openvpn).

Die Empfehlung ist 'no', wer es unbedingt braucht, weil er squid verwendet, der sollte prüfen, ob nicht ungewollt noch andere Funktionen dadurch beeinflusst werden.

1.3 OPT_LOGINUSER für C3SURF

Stellt eine pseudoechte Anmeldung für Benutzer bereit. Damit kann nicht mehr jeder das Internet oder die Dienste Deines Routers nutzen. Ich habe es so entwickelt, dass im laufenden Bertrieb eine Umschaltung erfolgen kann. Diese ist aber nicht implementiert.
Pseudoecht: es ist eben keine echte Benutzeranmeldung, aber die Software substituiert seit Version 2.1.0 jeden Benutzer auf eine Rechneradresse und handhabt das alles transparent. So wird nach Ablauf der Quota nicht der Rechner (IP-Adresse), sondern der Benutzer geblockt.

OPT_LOGINUSR Standard-Einstellung: `OPT_LOGINUSR='no'`

OPT_LOGINUSR='yes'
yes: echte Anmeldung verwenden (wird empfohlen)

LOGINUSR:
Stellt eine echte Anmeldung (User / Password) zur Verfügung. Die Account Pflege in der Config-Datei, stellt sicher, dass Passworte nur verschlüsselt übertragen werden.

LOGINUSR_DELETE_PERSISTENT_DATA
Standard-Einstellung: `LOGINUSR_DELETE_PERSISTENT_DATA='no'`

LOGINUSR_DELETE_PERSISTENT_DATA
Benutzerdaten auf einer Platte bleiben seit Version 2.1.0 erhalten. Der Standardwert 'no' stellt dies für die Accountdaten sicher.

Hinweise:
Mit der Eingabe von 'yes' kann die Funktion von früheren c3Surf-Versionen abgebildet werden. Alle Benutzer-Accounts werden dann beim Neustart gelöscht (wirklich alle). Danach erfolgt eine Neuanlage der Accounts, wie unten definiert. Das geschieht bei jedem Neustart, bis ein neues Router-Image auf den Router übertragen wird.

Es wird empfohlen hier 'no' beizubehalten. Dann bleiben die Daten zu den Accounts erhalten.

Dazu gehören:

- **Benutzer-Accounts**
- **Quota-Daten, wenn C3SURF_SAVE_QUOTA='yes' (Seite 8) gewählt ist (s.o.) (für einen einzelnen Account siehe: LOGINUSR_ACCOUNT_x_OVERWRITE (Seite 14))**

LOGINUSR_ACCOUNT_N `LOGINUSR_ACCOUNT_N='0'`

LOGINUSR_ACCOUNT_N
Anzahl Accounts, Wert: Ganze Zahl.
Gibt die Anzahl der User-Accounts an.

LOGINUSR_ACCOUNT_x_USER `LOGINUSR_ACCOUNT_x_USER='user1'`

LOGINUSR_ACCOUNT_x_USER
Username für die Anmeldung (Pflicht: ' ' also leer lassen ist unzulässig).

LOGINUSR_ACCOUNT_x_PWD `LOGINUSR_ACCOUNT_x_PWD='user1_secret'`

LOGINUSR_ACCOUNT_x_PWD
Passwort für die Anmeldung (Pflicht: ' ' also leer lassen ist unzulässig)

LOGINUSR_ACCOUNT_x_FORENAME `LOGINUSR_ACCOUNT_x_FORENAME='Vorname'`

LOGINUSR_ACCOUNT_x_FORENAME
Vorname des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

LOGINUSR_ACCOUNT_x_SURNAME `LOGINUSR_ACCOUNT_x_SURNAME='Nachname'`

LOGINUSR_ACCOUNT_x_SURNAME
Nachname des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

LOGINUSR_ACCOUNT_x_EMAIL `LOGINUSR_ACCOUNT_x_EMAIL='usr1@home.de'`

LOGINUSR_ACCOUNT_x_EMAIL
Email des Nutzers für die bessere Verwaltung (Optional, leer lassen erlaubt). Dieser Inhalt wird im Log und Admin-Interface angezeigt, so kann der Admin besser erkennen, wer gerade online ist.

LOGINUSR_ACCOUNT_x_OVERWRITE `LOGINUSR_ACCOUNT_x_OVERWRITE='yes'`

Optional:LOGINUSR_ACCOUNT_x_OVERWRITE
Überschreibe persistente Nutzerdaten beim Router-Neustart.

Hinweise:
Seit Version 2.1.0 kann ein Verzeichnis für persistente Daten angegeben werden. Dort werden die Daten für die Accounts gespeichert. Damit stehen diese Daten unverändert nach einem Reboot zur Verfügung. Mit dieser Option können der Benutzer-Account und alle zugehörigen persistenen Daten (Statistiken) überschrieben werden.

1.3.1 Optionale Parameter OPT_LOGINUSR

LOGINUSR_ACCOUNT_x_TIME `LOGINUSR_ACCOUNT_x_TIME='60'`

Optional:LOGINUSR_ACCOUNT_x_TIME
Anzahl der Minuten nur für diesen Nutzer, überschreibt C3SURF_TIME (Seite 8).

Siehe auch C3SURF_TIME (Seite 8). Fehlt dieser Parameter, so gilt C3SURF_TIME (Seite 8)
Das überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA='yes' (Seite 7) eingestellt ist.

LOGINUSR_ACCOUNT_x_BLOCKTIME `LOGINUSR_ACCOUNT_x_BLOCKTIME='240'`

Optional:LOGINUSR_ACCOUNT_x_BLOCKTIME
Sperrzeit nur für diesen Nutzer, überschreibt C3SURF_BLOCKTIME

Siehe auch C3SURF_BLOCKTIME (Seite 8). Fehlt dieser Parameter,
so gilt C3SURF_BLOCKTIME. Das überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA (Seite 7)='yes' eingestellt ist.

LOGINUSR_ACCOUNT_x_COUNTER `LOGINUSR_ACCOUNT_x_COUNTER='1'`

Optional:LOGINUSR_ACCOUNT_x_COUNTER
Anzahl der Anmeldungen nur für diesen Nutzer, überschreibt C3SURF_COUNTER.

Siehe auch C3SURF_COUNTER (Seite 7). Fehlt dieser Parameter, so gilt C3SURF_COUNTER (Seite 7). Das überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA='yes' (Seite 7) eingestellt ist.

1.4 Allgemeines

1.4.1 Web-Admin-Interface

Rechte: c3surf:view, admin

- view: Den Eintrag im Admin Menü anzeigen
- admin: Für die Nutzung der Funktionen im Web-Interface in httpd.txt einpflegen für Admins oder Nutzer die nicht über das Recht "all" vefügen, aber mit FreeSurf arbeiten sollen.

  Der fli4l-Admin mit dem Recht "all" sieht es sowieso und kann alles damit tun.
- Zu finden in Web-Admin unter Opt:
  - Als "c3Surf", wenn OPT_LOGINUSR (Seite 13)='no' (sprich: FreeSurf)
  - Als "LoginUsr", wenn OPT_LOGINUSR (Seite 13)='yes'

1.4.2 Was macht c3Surf

Du kannst ein Netz oder einzelne Hosts angeben, die nach dem Hochfahren zunächst gesperrt sind. Diese können dann über einen eigenen Web-Interface von den Benutzern selbst auf Zeit freigeschaltet werden. Dazu registriert sich der Benutzer formlos über das Web-Interface.

Ist die LOGINUSR - Option aktiviert, dann können sich nur Benutzer anmelden, die einen gültigen Account besitzen. Die Benutzernamen und Passworte pflegst Du.

Du kannst über das Admin-Interface Deines Routers die Benutzer sehen, ausloggen, temporär sperren oder die MAC-Adresse dauerhaft sperren. Die Sperrung betrifft immer nur die Anmeldung über c3Surf und wird von c3Surf verwaltet. Kommt der Rechner über eine andere NIC an Deinen Router, hat die Sperre keine Wirkung.

Die Anmeldung erfolgt durch Vornamen, Namen und E-Mailadresse oder durch User/Passwort. Nach Ablauf einer eingestellten Zeit wird der Zugang wieder gesperrt und kann durch neue Anmeldung wieder freigeschaltet werden.

Du kannst die Anmeldeseite auch für die Benutzer sperren (siehe FreeSurf bzw. LoginUsr im OPT-Menue des Web-Interfaces).

Du kannst das alles im Admin-Web-Interface nachvollziehen.

Willst Du bestimmte Rechner dauerhaft freischalten, so kannst Du dies im Web-Interface tun. Siehe dazu die ARP-Liste oder die DHCP-Leases.

Jede Nutzung kann seit Version 2.1.0 mit Quotas versehen werden. Damit kann die Nutzung in der Zeit eingeschränkt werden. Mit den Parametern "-TIME", "-BLOCKTIME" und "-COUNTER" lässt sich dabei sehr viel einstellen, auch benutzerbezogen.

Beispiele:

Time	BLocktime	Counter	Ergibt Quota, wenn C3SURF_QUOTA='yes'
60	-1	0	60 Min Zeit, keine Sperre nach Ablauf, mit jeder Anmeldung läuft die Zeit (Parkuhrprinzip) (C3SURF-Verhalten wie vor der Version 2.1.0, da gab es diese Steuerungsoptionen noch nicht)
60	240	0	60 Min Zeit, danach für 240 gesperrt, mit jeder Anmeldung läuft die Zeit (Parkuhrprinzip = Geld rein, Zeit läuft ohne Unterbrechungsmöglichkeit)
60	0	-1	60 Min Zeit, nach Ablauf der Zeit wird der Zugang bis 00:00 Uhr gesperrt, beliebige An- Abmeldungszahl (kein Parkuhrprinzip)
60	-1	1	60 Min Zeit, keine Sperre nach Ablauf der Zeit, die Zeit kann 1x unterbrochen werden
60	-1	-1	60 Min Zeit, keine Sperre nach Ablauf der Zeit, beliebig viele Unterbrechungen möglich

1.4.3 Systemanforderungen

Wichtig: *Nicht für Version 3.0.x oder frühere.*

1.5 Sonstiges

1.5.1 WARNUNG

Wichtig: *Ohne OPT_LOGINUSR='yes' (Seite 13) ist es jeder Person möglich, die für ihren Rechner eine IP-Adresse vom Router zugewiesen bekommen hat (z. B. aus einem offenen WLAN), einen freien Zugriff auf das Internet und die Dienste Deines Routers, die Du nicht geblockt hast, zu bekommen. c3Surf unterstützt beim Blocken der Dienste, ist aber kein Ersatz für eine "ordentliche" Konfiguration der Firewall in der "base.txt".*

1.5.2 Empfehlung

Wichtig: *Achte darauf, dass Du Deinen Router mit einer "Recovery-Version" versehen hast - für alle Fälle. Ich habe die zwar noch nicht gebraucht, aber sicher ist sicher. Mit einer unglücklichen Konfiguration kannst Du Dich komplett aussperren.*

1.5.3 Probleme, Änderungen und Fehler

Änderungen, die Du gemacht hast, schickst Du mir bitte mit einer kurzen Beschreibung. Ich verspreche, dass ich die Änderungen bei Gefallen in das nächste Release übernehme.

Falls gar nix läuft :
Fehlerbeschreibung erstellen, mit Config-Info und `mailto: c3surf@arcor.de`. Oder die fli4l-Foren nutzen, ich lese diese.

1.5.4 Lizenz

Ich stelle diese meine Arbeit unter "GNU" General Public License in Version 2 oder folgende. Damit ist diese Software frei für Benutzer, Entwickler und Firmen. Es ist guter Stil, wenn Urheber in einer weiteren Verwertung oder Veröffentlichung genannt werden. Das gilt besonders für freie Werke.
- - - - - - -
This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

Please Name the author, if you use C3SURF or parts of it in your own work.

1.5.5 Spenden

PayPal: c3surf@arcor.de

Ich habe viel meiner Zeit investiert, das war diese Software mir wert. Wenn Dir die Software etwas wert ist, freue ich mich über eine Spende.

Das ist absolut freiwillig. Die Software steht jedem frei zur Verfügung. Ebenso das Verlangen etwas spenden zu wollen.

1.6 Literatur

Wer gerne sein Netz für andere zur Verfügung stellt, der sollte sich auch einmal mit der rechtlichen Situation auseinander setzen.

Es gibt eine unter CC stehende Arbeit dazu:
Rechtsfragen offener Netze:
http://digbib.ubka.uni-karlsruhe.de/volltexte/1000007749
Autor: Mantz, Reto
Reihe: Schriften des Zentrums für Angewandte Rechtswissenschaft / ZAR
Zentrum für Angewandte Rechtswissenschaft, Universität Karlsruhe (TH)
Band: 8
Verlag: Universitätsverlag Karlsruhe
ISBN: 978-3-86644-222-1
Erschienen: 10.04.2008

A Anhang zum 3csurf Paket

A.1 Wie ist C3SURF entstanden

Meine alten Rechner konnten nur WLAN WEP Verschlüsselung mit 48bit. Da kann ich auch gleich ein offenes, nicht verschlüsseltes WLAN betreiben. Aber ich möchte schon wissen wer das Netz bei mir nutzt. Also brauchte ich ein Paket, welches eine formlose Registrierung in meinem Netz ermöglicht. Pate stand "opt_onco" (onco is Copyright (c) 2001-2007 Michael Mattes), einen Dank an Ihn als Ideenlieferant für mich. Jedoch fehlte mir dort die eigene Registrierung durch den Benutzer. Also baute ich etwas drum herum. Später dann ein eigenes "opt_c3surf". Was eigentlich opt_3surf heißen (sprich: FreeSurf) sollte. Doch als das Paket fertig gebaut war, scheiterte das '3surf' an den fli4l-Namenskonventionen. Da hatte ich viel Spass bei der Überarbeitung.

Später erweiterte ich es um die OPT_LOGINUSR Option. Seitdem kann eine "fast" echte Anmeldung nachgestellt werden.

A.1.1 Opt-C3SURF Team

Creation:	07. Januar 2008	Frank Saurbier	mailto: c3surf@arcor.de
Doku-Text:	07. Januar 2008	Frank Saurbier	mailto: c3surf@arcor.de
Doku-Format:	01. April 2009	Helmut Backhaus	mailto: helmut.backhaus@gmx.de
Last update:	8. Juli 2009	Frank und Helmut	

A.2 Andere Opt's und Howto

A.2.1 cpmvrmlog Config

Beispiel für das C3SURF-Logverzeichnis, mit restart des mini_httpd

```
# archive C3SURF log dir
# einmal im Monat am 1. um 01:30
# maximal 12 Archive aufbewahren
CPMVRMLOG_n_ACTION='move'
CPMVRMLOG_n_SOURCE='/var/log/c3surf/c3surf_*.log'
CPMVRMLOG_n_DESTINATION='/data/Archive/log/c3surf'
CPMVRMLOG_n_CUSTOM='/usr/local/bin/c3surf_kill_httpd.sh'
CPMVRMLOG_n_MAXCOUNT='12'
CPMVRMLOG_n_CRONTIME='30 1 1 * *'
```

A.2.2 Samba ohne Anmeldung erlauben

Man nehme das opt_usercmd und trage dort folgendes ein.

```
USERCMD_BOOT_N='3'
USERCMD_BOOT_1='/sbin/iptables -I c3surf\_control 1 -v -p udp --dport
                137:138 -j RETURN' # samba thru c3surf
USERCMD_BOOT_2='/sbin/iptables -I c3surf\_control 1 -v -p tcp --dport
                455 -j RETURN'     # samba thru c3surf
USERCMD_BOOT_3='/sbin/iptables -I c3surf\_control 1 -v -p tcp --dport
                139 -j RETURN'     # samba thru c3surf
```

Durch hinzufügen der Option "-d IPsambaHOST" in den oberen Zeilen, kann die jeweilige Regel noch um den Zielrechner erweitert werden.

Damit werden die Samba Ports normal durch die Forward-Chain geleitet und nicht mehr von C3SURF geblockt. Solltest Du in der Forward-Chain samba Weiterleitungen verbieten, so ändern diese Eintragungen nichts daran.

Es gelten also immer noch die Einstellungen Deiner base.txt.

Index