

Package C3SURF - Zugangskontrolle Version 2.3.1

für den FLI4L Version 3.3.X

Das C3SURF-Team

Idee und Entwicklung

Frank Saurbier

<mailto:c3surf@arcor.de>

Dokumentationsbearbeitung

Helmut Backhaus

<mailto:helmut.backhaus@gmx.de>

16. September 2009

Inhaltsverzeichnis

1	Dokumentation des Paketes C3SURF	3
1.1	Kurzbeschreibung des Opt's	3
1.2	Hinweise zur Installation	3
1.3	Config Datei und die Parameter	5
1.3.1	Optionale Parameter OPT_C3SURF	14
2	Dokumentation des Paketes LOGINUSR für C3SURF	15
2.1	Konfiguration OPT_LOGINUSER für C3SURF	15
2.1.1	Optionale Parameter OPT_LOGINUSR	17
3	Dokumentation des Paketes VOUCHER für C3SURF	19
3.1	Konfiguration von OPT_VOUCHER	19
3.1.1	Optionale Parameter OPT_VOUCHER	21
4	Dokumentation des Paketes Traffic für C3SURF	24
4.1	Konfiguration OPT_C3SURF_TRAFFIC	24
5	Allgemeines zu C3SURF	26
5.1	Web-Admin-Interface	26
5.2	Was macht c3Surf	26
5.3	Systemanforderungen	27
6	Sonstiges zu C3SURF	28
6.1	WARNUNG	28
6.2	Empfehlung	28
6.3	Probleme, Änderungen und Fehler	28
6.4	Lizenz	28
6.5	Spenden	29
6.6	Literatur	29
A	Anhang zum C3SURF Paket	30
A.1	Wie ist C3SURF entstanden	30
A.2	Opt-C3SURF Team	30
A.3	Andere Opt's und Howto	31
A.3.1	cpmvrnlog Config	31
A.3.2	Samba ohne Anmeldung erlauben	31

1 Dokumentation des Paketes C3SURF

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.

1.2 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.

Wichtig: Der `fli4l` muss als DNS-Server bei den Clients eingetragen sein und muss befähigt sein Namen aufzulösen. Dazu

- benötigt er einen "Forward" auf den DNS-Server des Netzes oder
- er ist selbst der DNS-Server und kann ggf. automatisch Verbindungen aufbauen.

Sonst gibt es Probleme automatisch auf die Anmeldeseite umzuleiten. Die kann aber immer noch manuell durch die Eingabe ihrer URL aufgerufen werden.

- Migration zur Version 2.3.1 (von 2.3.0)
 - Pflege der neue Variablen. Da es sich nur um optionale Variablen handelt, ist die Pflege nicht zwingend erforderlich. Der neue Bereich ist in der `config.txt` so
 - `"# + new 2.3.1 + begin ————— delete this line"` gekennzeichnet.
 - Das Voucherformat hat sich geändert, alte Voucher können weiter verbraucht werden, sie werden aber bei der Generierung von neuen Vouchern nicht als existent erkannt. Wer es sauber haben will, sollte alle Voucher löschen und dann neu erzeugen.

- Migration zur Version 2.3.0 (von 2.2.2)
 - Will man keine Gutscheine nutzen, sind keine Änderungen an der Konfiguration nötig.
 - Pflege die neue Variablen für das OPT_C3SURF_VOUCHER, sofern man die Gutscheinfunktion nutzen möchte.
 - Der neue Bereich ist in der config.txt so
 - "# + new 2.3.0 + begin ————— delete this line" gekennzeichnet.
- 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_ARP " in 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.

1.3 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 Einzelnen 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 15) 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 31)

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

Definiert das Verzeichnis, 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 16) kann das überschreiben der entsprechenden Benutzerdaten erzwungen werden.

Mittels `LOGINUSR_DELETE_PERSISTENT_DATA='yes'` (Seite 15), 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 9) 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 9) noch verbliebene Differenz von der Anmeldung davor.

Ist zudem [C3SURF_BLOCKTIME='0'](#) (Seite 9) gewählt, so wird der [C3SURF_COUNTER](#) (Seite 8) erst nach 0:00 Uhr des Folgetages zurückgesetzt.

- Mit C3SURF_COUNTER='0'
entspricht der Wert dem Parkuhrprinzip (Geld rein, Geld weg, Zeit läuft: also keine Unterbrechungen möglich) und bildet das Verhalten von C3SURF vor der Version 2.1.0 ab.
- Mit C3SURF_COUNTER='1'
wird diese Funktion abgeschaltet = beliebig viele Unterbrechungen der Freiminuten sind möglich.
- Mit C3SURF_COUNTER='2'
gibt es beliebig viele Unterbrechungen (wie '1'), aber die Blockzeit wird bereits mit der ersten Anmeldung heruntergezählt. Im Gegensatz zur '1', wo die Blockzeit erst nach dem Verbrauch der gesamten Zeit eingestellt wird.

Damit kannst Du z. B. 10 Stunden Onlinezeit ([C3SURF_TIME='600'](#)) (Seite 9) mit einer Blockzeit von einer Woche ([C3SURF_BLOCK_TIME='10080'](#) (Seite 9) : 60sec x 24h x 7Tage) kombinieren. Dann können die 10 Stunden innerhalb einer Woche verbraucht werden. Wer sie am ersten Tag am Stück verbraucht, der wartet dann eben den Rest der Woche. Nach Ablauf der Blockzeit werden wieder 10 Stunden bereitgestellt.

Kurzfassung: Der Nutzer hat ein Wochenkontingent von 10 Stunden, welches er sich selbst sinnvoll auf die Woche verteilen kann. Verbraucht er das Kontingent langsamer, dann wird er nicht mit einem "Quota-Block" belegt. Es entsteht dann keine Wartezeit.

Gilt auch für [LOGINUSR_ACCOUNT_x_COUNTER](#) (Seite 17).

Empfehlung: [C3SURF_SAVE_QUOTA='yes'](#) (Seite 9), dann bleiben die Werte auch nach einem normalen Neustart erhalten.

Bei Stromausfall gehen die Werte verloren.

Ist [C3SURF_QUOTA='yes'](#) (Seite 7), so wird nach der Überschreitung des Zählers die Sperre entsprechend [C3SURF_BLOCKTIME](#) (Seite 9) aktiviert.

C3SURF_TIME Standard-Einstellung: C3SURF_TIME='60'

Anzahl der Minuten, die eine Freischaltung gilt.

Wobei der Wert '0' ein unlimitedes Login bedeutet (gilt auch für LOGINUSR_ACCOUNT_x_TIME).

Sonderfall:

- C3SURF_TIME='0'

Bedeutet eine unlimitede Onlinezeit. Der Nutzer sollte sich selbst abmelden. Das System (C3SURF) meldet ihn nur ab, wenn der Rechner abgeschaltet wird und C3SURF_CHECK_ARP='yes' (Seite 9) (Standardeinstellung) gewählt wurde.

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:

- C3SURF_BLOCKTIME='0'
es erfolgt eine Sperrung der Adresse, bzw. des Nutzers bis 00:00 Uhr des Folgetages.
- C3SURF_BLOCKTIME='-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 15), 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 10). 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 (fi4l) 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 10). Wieviele und welche explizit benannten Ports sollen von c3Surf permanent geblockt werden? Es gibt dann keinen Zugriff auf die dahinter stehenden Dienste des Routers (fi4l) 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_MTGAPRI)
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.
```

1.3.1 Optionale Parameter OPT_C3SURF

C3SURF_CONTROL_SQUID Standard-Einstellung: C3SURF_CONTROL_SQUID='no'

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.

C3SURF_SLOPPY_MAC Standard-Einstellung: C3SURF_SLOPPY_MAC='no'

- C3SURF_SLOPPY_MAC='no'
(Standard), wenn dieser Parameter nicht angegeben wurde, lasse Login nur mit MAC-Adressermittlung aus der ARP-Tabelle zu. Es wird also nicht 'schlampig' mit MAC-Adressen verfahren.
- C3SURF_SLOPPY_MAC='yes'
Dann nimmt C3SURF es mit der MAC-Adresse nicht so genau, sollte diese fehlen und nicht über die ARP-Tabelle ermittelbar sein, so wird trotzdem die Anmeldung erlaubt. Wer hier 'yes' wählt sollte [C3SURF_CHECK_ARP='no'](#) (Seite 9) setzen. Sonst erfolgt die automatische Abmeldung (im Mittel nach einer Minute), weil der "countdown"-Prozess wegen fehlendem Eintrag in der ARP-Tabelle zur Abmeldung aufgefordert wird.

C3SURF_CHECK_CURFEW Standard-Einstellung: C3SURF_CHECK_CURFEW='yes'

- C3SURF_CHECK_CURFEW='no'
schalte automatisches Abmelden beim Erreichen der Sperrstunde ab.
- C3SURF_CHECK_CURFEW='yes'
(Standard), wer bei Erreichen der Sperrstunde angemeldet ist, wird rausgeworfen.

C3SURF_PORTAL_DEFAULT_LANG Standard-Einstellung: C3SURF_PORTAL_DEFAULT_LANG='de'

Wertebereich: ein zweistelliger Ländercode (z. B. 'de', 'es', 'en').

Legt die Standard-Sprache für die Anmeldeseite fest. Wird diese Variable weggelassen wird 'de' angenommen.

Es sollte unter ~/opt/files/srv/www/c3surf/lang/ eine Datei namens c3surf.<ländercode> existieren. Mit der Version 2.3.1 werden c3surf.de, c3surf.en und c3surf.es mitgeliefert. Wer daraus für eine andere Sprache eine weitere Datei erstellt, möge mir diese schicken.

C3SURF_PORTAL_LANGUAGES

Standard-Einstellung: C3SURF_PORTAL_DEFAULT_LANG='de es en it'

Wertebereich: eine mit Leerzeichen getrennte Liste von immer zwei Buchstaben.

Legt fest, welche Sprachdateien für die Anmeldeseite auf das System übertragen werden sollen. Sollten hier zweistellige Kürzel stehen, zu denen keine Sprachdatei existiert, so wird bei der Generierung der Router-Images eine Warnung ausgegeben, dass zu dem Kürzel in der Liste keine Datei gefunden wurde und somit auch nichts kopiert wurde. Der Build-Prozess wird nicht abgebrochen.

2 Dokumentation des Paketes LOGINUSR 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 Betrieb 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.

2.1 Konfiguration OPT_LOGINUSER für C3SURF

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 9) gewählt ist (s.o.) (für einen einzelnen Account siehe: `LOGINUSR_ACCOUNT_x_OVERWRITE` (Seite 16))

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 persistenten Daten (Statistiken) überschrieben werden.

2.1.1 Optionale Parameter OPT_LOGINUSR

LOGINUSR_ACCOUNT_x_TIME LOGINUSR_ACCOUNT_x_TIME='60'

Anzahl der Minuten nur für diesen Nutzer, überschreibt C3SURF_TIME (Seite 9).

Siehe auch C3SURF_TIME (Seite 9). Fehlt dieser Parameter, so gilt C3SURF_TIME (Seite 9). Das Überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA='yes' (Seite 7) eingestellt ist.

LOGINUSR_ACCOUNT_x_BLOCKTIME LOGINUSR_ACCOUNT_x_BLOCKTIME='240'

Sperrzeit nur für diesen Nutzer, überschreibt C3SURF_BLOCKTIME

Siehe auch C3SURF_BLOCKTIME (Seite 9). Fehlt dieser Parameter, so gilt C3SURF_BLOCKTIME. Das überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA='yes' (Seite 7) eingestellt ist.

LOGINUSR_ACCOUNT_x_COUNTER LOGINUSR_ACCOUNT_x_COUNTER='1'

Anzahl der Anmeldungen nur für diesen Nutzer, überschreibt C3SURF_COUNTER.

Siehe auch C3SURF_COUNTER (Seite 8). Fehlt dieser Parameter, so gilt C3SURF_COUNTER (Seite 8). Das Überschreiben macht natürlich nur Sinn, wenn C3SURF_QUOTA='yes' (Seite 7) eingestellt ist.

LOGINUSR_ACCOUNT_x_CURFEW LOGINUSR_ACCOUNT_x_CURFEW='Liste Sperrstunden'

Format: (Liste von Sperrstunden 0-23 durch Leerzeichen getrennt)

Beispiele:

LOGINUSR_ACCOUNT_x_CURFEW='0 1 2 3 4 5 6 7 21 22 23'

Bedeutung: Eine Anmeldung ist nur zwischen 8:00-20:59 Uhr erlaubt. Die Anmeldung wird immer unterbunden, wenn der Nutzer sich innerhalb der Stunde (plus 0-59 Minuten), die in der Liste steht, versucht anzumelden.

Ist der Benutzer angemeldet und läuft in die Sperrstunde, so wird er ohne Warnung automatisch abgemeldet. Das Abmeldeverhalten kann durch den optionalen Parameter [C3SURF_CHECK_CURFEW](#) (Seite 14)='no' unterbunden werden.

Mit dieser Liste kann ein Zugang sehr flexibel eingeschränkt werden. Die Liste kann auch wie gewohnt im Webinterface gepflegt werden. Bei der Eingabe findet keine Prüfung der Liste statt. **Es sind nur die Zahlen von 0 bis 23 sinnvoll! Du achtest selbst auf das richtige Format.**

Zugehöriger OPT_C3SURF Parameter:

[C3SURF_CHECK_CURFEW](#) (Seite 14)='no'

- C3SURF_CHECK_CURFEW='no'
schalte automatisches Abmelden beim Erreichen der Sperrstunde ab.
- C3SURF_CHECK_CURFEW='yes'
(Standard), wer bei Erreichen der Sperrstunde angemeldet ist, wird rausgeworfen.

3 Dokumentation des Paketes VOUCHER für C3SURF

Das OPT_C3SURF_VOUCHER ermöglicht einen anonymen Zugang in das Internet. Es werden Gutscheine erstellt, die in unterschiedlichen Kategorien eingerichtet werden können. Das Opt kann dann über das Web-Admin-Interface manuell oder automatisch verwaltet werden.

3.1 Konfiguration von OPT_VOUCHER

OPT_C3SURF_VOUCHER OPT_C3SURF_VOUCHER='no'

Das Opt C3SURF_VOUCHER benutzen ('yes'), Standard ist 'no'. Es soll das Gutscheinsystem von C3SURF verwendet werden. Gutscheine sind anonyme aber sichere Einmal-Accounts, die zur Anmeldung verwendet werden können. Voraussetzung ist die Einstellung "[OPT_LOGINUSR='yes'](#)" (Seite 15).

Die Erzeugung und Löschung der Gutscheine übernehmen zwei nächtliche cron JOBS, welche jederzeit auch manuell(Admin-Interface) gestartet werden können. Weiter unten erfährst Du, wie Du diese Jobs selbst einplanen oder komplett abschalten kannst. So kannst Du entscheiden, ob alles automatisch und zu welcher Zeit ablaufen soll oder ob Du es lieber manuell aus dem Admin-Interface des fli4l heraus erledigst.

Alle neu generierten Gutscheine werden an eine Druckliste angehängt. Nur in der Druckliste ist das zum Gutschein gehörende Kennwort im Klartext gespeichert. Du kannst diese Liste jederzeit Herunterladen, Drucken oder Löschen. Nach dem Löschen der Liste, kann das Kennwort nicht wieder ermittelt werden. Der normale Ablauf ist, zuerst die Liste drucken und dann die Liste löschen. Es liegt in Deiner Verantwortung dafür zu sorgen, dass es immer nur ein gedrucktes Exemplar eines Gutscheines gibt. Die implementierte Druckfunktion ist rudimentär in html implementiert. Es wird keine Rücksicht auf Seitenumbruch genommen. Ehrlich gesagt weiß ich nicht, ob es überhaupt möglich ist im html darauf zu reagieren, da es sich um eine Beschreibungssprache für Bildschirmpräsentation handelt. Da sind gute Vorschläge oder Ratschläge an mich willkommen. Die Gutscheine, die dem Seitenwechsel zum Opfer fallen, kannst Du ja einfach vernichten. Das Verfallsdatum eines Gutscheines erledigt dann ja irgendwann den Rest. Oder du lädst die Liste herunter und löscht sie dann. Mit der heruntergeladenen Liste könntest Du mittels Tabellenkalkulation oder Textverarbeitung (Serienbrief) ein eigenes schönes Layout erstellen, welches dann auch Seitenwechsel sauber berücksichtigt. Wenn Du da etwas schönes erstellt hast, schicke es mir an c3surf@arcor.de. Ich würde es dann in das nächste Paket, natürlich unter Deinem Namen, im source Ast veröffentlichen. Ich habe es noch nicht gemacht, da ich das Gutscheinsystem von C3SURF selbst nicht benötige.

C3SURF_VOUCHER_N C3SURF_VOUCHER_N='n'

Wertebereich: 0 und Natürliche Zahlen

Es wird angegeben, wie viele verschiedene Gutscheinkategorien erzeugt werden sollen. Wichtigstes Kriterium für Gutscheine ist die Zeit, die man damit angemeldet bleiben kann. Daneben gibt man noch die Anzahl der Gutscheine und deren Gültigkeit in Tagen an. Siehe auch die folgenden Variablen.

C3SURF_VOUCHER_x_TIME C3SURF_VOUCHER_x_TIME='30'

Wertebereich: Natürliche Zahlen

Beispiel: Gutscheine der Kategorie 'n' sind für 30 Minuten ausgelegt.

Hier gibst Du die Anzahl der Minuten für einen Gutschein dieser Kategorie ('n' siehe oben) an.

C3SURF_VOUCHER_x_COUNT C3SURF_VOUCHER_x_COUNT='3'

Wertebereich: Natürliche Zahlen

Beispiel: Es werden insgesamt 3 Gutscheine für diese Zeitkategorie erzeugt.

Hier gibst Du an, wieviele Gutscheine dieser Kategorie erzeugt werden sollen.

C3SURF_VOUCHER_x_DAYS C3SURF_VOUCHER_x_DAYS='90'

Wertebereich: 0 und Natürliche Zahlen

Beispiel: Diese Gutscheine sind 90 Tage nach der Erzeugung gültig.

Hier gibst Du an, wie viele Tage ein solcher Gutschein ab seiner Erzeugung gültig sein soll. Daraus erzeugt C3SURF bei der Generierung ein Verfallsdatum für diesen Gutschein. Entsprechende Jobs sorgen für die Löschung, oder du wählst die manuelle Variante. Ein Gutschein erlischt normalerweise früher, nämlich dann, wenn er das erste Mal verwendet wird.

Wichtig: "0" bedeutet, dass Gutscheine dieser Kategorie kein Verfallsdatum haben. Diese werden erst mit Benutzung ungültig oder wenn die Zeit komplett verbraucht wurde (wird auch durch C3SURF_VOUCHER_LIVES_n beeinflusst). Löschen kannst Du sie aber jederzeit im Admin-Interface des fli4l.

3.1.1 Optionale Parameter OPT_VOUCHER

C3SURF_VOUCHER_x_LIVES C3SURF_VOUCHER_x_LIVES='n'

Wertebereich(n): -1, 0, Natürliche Zahlen

Angabe von Stunden, die der Voucher noch nach der ersten Anmeldung weiterlebt.

Sonderfälle:

- C3SURF_VOUCHER_x_LIVES='-1'
Lebt bis zum ursprünglich generierten Verfallsdatum aus C3SURF_VOUCHER_DAYS weiter.
- C3SURF_VOUCHER_x_LIVES='0'
(Standard), bedeutet Voucher wird mit erster Anmeldung ungültig.
- C3SURF_VOUCHER_x_LIVES='Natürl. Zahl'
Anzahl der Stunden, die der Voucher weiterlebt nach erster Anmeldung - ggf. ein neues Verfallsdatum berechnen.

Diese Gutscheine werden nicht mit der ersten Anmeldung ungültig, sondern leben 'n' Stunden weiter. Sobald der Gutschein benutzt wird, wird daraus ein zeitlich limitierter LOGINUSR-Account generiert oder es wird das Verfallsdatum des Vouchers neu berechnet. Dieser Account / Voucher darf sich beliebig oft an und wieder abmelden. Es wird das von LOGIN_USR gewohnte Quota-System für diesen Account verwendet. Erst wenn die gesamte Zeit verbraucht ist oder wenn das Verfallsdatum (C3SURF_VOUCHER_DAYS_n) erreicht wurde, wird dieser Account automatisch von C3SURF gelöscht.

C3SURF_VOUCHER_DEL_CRON C3SURF_VOUCHER_DEL_CRON='0 4 * * *'

Wertebereich: 'cron-Syntax' oder 'never'

Der oben angegebene Wert ist der Standard, wenn diese Variable in der config-Datei 'c3surf.txt' fehlt. Standard: lösche täglich morgens um 4 Uhr alle verfallenen Gutscheine.

Die cron-Syntax ist einzuhalten, wird nicht geprüft. Zusätzlich kann der Wert 'never' verwendet werden. Dann wird der Job vom System überhaupt nicht eingeplant. Du kannst im Admin-Interface jederzeit manuell alle verfallenen Gutscheine löschen lassen.

C3SURF_VOUCHER_GEN_CRON C3SURF_VOUCHER_GEN_CRON='15 4 * * *'

Wertebereich: 'cron-Syntax' oder 'never'

Der oben angegebene Wert ist der Standard, wenn diese Variable in der config-Datei 'c3surf.txt' fehlt. Standard: generiere täglich morgens um 4:15 Uhr neue Gutscheine, falls weniger als C3SURF_VOUCHER_COUNT vorhanden sind.

Die cron-Syntax ist einzuhalten, wird nicht geprüft. Zusätzlich kann der Wert 'never' verwendet werden. Dann wird der Job vom System überhaupt nicht eingeplant. Du kannst im Admin-Interface jederzeit manuell neue Gutscheine bis zur Menge [C3SURF_VOUCHER_x_COUNT](#) (Seite 20) erzeugen lassen.

Alle neu generierten Gutscheine werden an eine Druckliste angehängt. Nur in der Druckliste ist das zum Gutschein gehörende Kennwort im Klartext gespeichert. Sorge selbst dafür, dass jeder Gutschein nur einmal gedruckt wird, indem Du die Liste sofort nach dem Ausdruck oder Herunterladen löscht. Lasse Unbefugte nicht an die Liste herankommen.

C3SURF_VOUCHER_PRTUPDATE Standard-Einstellung: C3SURF_VOUCHER_PRTUPDATE='no'

Wertebereich: 'yes' oder 'no'

Aktualisierung der Druckdatei. Meine Empfehlung: 'no'. Wer wenige Gutscheine im System hält und die Druckdatei nach dem Ausdruck oder Herunterladen nicht löschen möchte, der kann mit 'yes' eine Aktualisierung der Druckdatei beim Verbrauch von Gutscheinen einstellen. Bei der Wahl von 'yes' werden benutzte Gutscheine auch aus der Druckdatei gelöscht. Das benötigt Ressourcen auf dem Router.

C3SURF_VOUCHER_USRLEN Standard-Einstellung: C3SURF_VOUCHER_USRLEN='12'

Wertebereich: '1-16'

Zeichenlänge für Gutscheinaccount festlegen, ab 8 Zeichen werden '-' als Trenner eingebaut, die auch eingegeben werden müssen. Es werden immer vier Zeichen gruppiert. Der Maximalwert ist 16.

C3SURF_VOUCHER_USRCAP Standard-Einstellung: C3SURF_VOUCHER_USRCAP='random'

- 'yes' : nur Großbuchstaben
- 'no' : nur Kleinbuchstaben
- 'random' : zufällige Wechsel von Groß- Kleinschreibung (Empfehlung)

Mit dieser Variable wird festgelegt ob Groß- oder Kleinbuchstaben im Benutzernamen verwendet werden sollen. Der Wert "random" (empfohlen) bewirkt eine zufällige Auswahl.

C3SURF_VOUCHER_PWDLEN Standard-Einstellung: `C3SURF_VOUCHER_PWDLEN='6'`

Wertebereich: 1-12

Zeichenlänge für das Gutschein-Password.

C3SURF_VOUCHER_PWDMOD Standard-Einstellung: `C3SURF_VOUCHER_PWDMOD='3'`

Wertebereich: 1-5

Modulo für zufällige Verlängerung des Passwortes. Max: 5 (die Werte 0, 1, 2, 3, 4), Min 1 (der Wert 0). Es wird bei der Password-Generierung das Password zufällig um die möglichen Werte verlängert. Damit ergeben sich per default Password-Längen zwischen 6 und 8. Maximal einstellbar sind Password-Längen zwischen 12 und 16, das ist sicher genug mit zufälliger Groß- und Kleinschreibung.

C3SURF_VOUCHER_PWDCAP Standard-Einstellung: `C3SURF_VOUCHER_PWDCAP='random'`

- 'yes' : nur Großbuchstaben
- 'no' : nur Kleinbuchstaben
- 'random' : zufällige Wechsel von Groß- Kleinschreibung (Empfehlung)

Mit dieser Variable wird festgelegt ob Groß- oder Kleinbuchstaben im Passwort verwendet werden sollen. Der Wert "random" (empfohlen) bewirkt eine zufällige Auswahl.

4 Dokumentation des Paketes Traffic für C3SURF

Das OPT_C3SURF_TRAFFIC ermöglicht "Power User" auszubremsen und in ihre Schranken zu weisen. Es wird das Datenvolumen in einem definierbaren Zeitintervall überwacht und ausgewertet. Das ganze ist etwas rudimentär, kann aber nach eigenen Bedürfnissen konfiguriert werden.

4.1 Konfiguration OPT_C3SURF_TRAFFIC

OPT_C3SURF_TRAFFIC Standard-Einstellung: OPT_C3SURF_TRAFFIC='no'

Wer das Traffic-Modul aktivieren möchte, der trägt hier 'yes' ein. Dann wird eine Pflege den noch folgenden Variablen nötig. Die Defaultwerte sind für eine großzügige Auslegung (siehe hier beschriebenes Beispiel) bei einem DSL-6000 Anschluss ausgelegt.

Mit OPT_C3SURF_TRAFFIC wird ein rudimentäres Modul zum Schutz vor Langzeit-Powersaugern bereitgestellt. Mit den folgenden Variablen kann eingestellt werden in welcher Zeit welches Datenvolumen nicht überschritten werden darf. Dabei wird nicht zwischen up- und download unterschieden. Die Logik dieses Moduls ist so konzipiert, dass bei zweimaliger Überschreitung des Volumens in Folge die Abmeldung des Verursachers erfolgt und dieser mit der definierten Zeitstrafe (Blockzeit) belegt wird. Diese Einstellungen wirken global für alle C3SURF-Benutzer. Die Wahl der richtigen Parameter hängt natürlich von der vor Ort verfügbaren Bandbreite ab. Da keine Sperre bei einmaliger Überschreitung erfolgt, kann auch mal ein Betriebssystem-Update oder das normale herunterladen größerer Datenmengen erfolgen. Sollte der Verbrauch der Bandbreite aber als "dauerhaft" erkannt werden, hat das Konsequenzen. Die Begrenzung sollte jedoch immer an die individuellen Bedürfnisse angepasst werden. Es geht in diesem Modul darum, die Langzeit-Bandbreitenvernichter zu tadeln.

Will man beispielsweise das gelegentliche Herunterladen von größeren Datenmengen erlauben, so muss bei der Wahl der Parameter aus der erlaubten Datenmenge und der verfügbaren Bandbreite eine Zeit kalkuliert werden, in der die Datenmenge herunterladbar sein soll.

Beispiel:

Will man das gelegentliche Herunterladen einer Distributions-CD erlauben (700MB) so würde das im günstigsten Fall folgende Zeiten in Anspruch nehmen:

DSL-	1000	ca.	93	Minuten
DSL-	2000	ca.	47	Minuten
DSL-	6000	ca.	16	Minuten
DSL-	16000	ca.	6	Minuten

Ohne Erfahrungswerte zu haben würde ich vorschlagen die prognostizierte Zeit für das Datenvolumen als Messpunkt für die Zeit zu nehmen. Die erlaubte Datenmenge (hier 700MB) sollte durch einen Wert kleiner 2 aber größer 1 geteilt werden. Beginnen würde ich mit Werten nahe bei 2. Wer hier Erfahrungen gesammelt hat und/oder einen guten Vorschlag für eine Berechnung hat, möge mir die Daten zukommen lassen. Ich verwerte diese dann in künftigen Verbesserungen der Dokumentation.

Beispiel (konservativ): $700\text{MB} / 1,9 = 386317473 \text{ Bytes}$

Das wäre die Anzahl Bytes, die in der oben kalkulierten Zeit maximal heruntergeladen werden darf. Ob es sinnvoll ist, solch ein hohes Volumen bei DSL-1000 oder DSL-2000 pro Nutzer zuzulassen, hängt auch von der Anzahl der erwarteten Nutzer ab.

Will man solche Datenmengen nicht zulassen, sondern maximal z. B. das Musikhören eines mp3-Streams oder einen kontinuierlichen Datenstrom von 128 kBit/s erlauben, so sollte man unabhängig vom DSL-Anschluss folgende Werte wählen: 16220160 Bytes pro 15 Minuten (ergibt sich aus $128\text{kBit/s} * 1024 / 8\text{Bit} = 16384 \text{ Bytes/s} * 60 = 983040 \text{ Bytes/min} * 15\text{min} = 14745600 \text{ Bytes} * 1,1 = 16220160 \text{ Bytes (pro 15 min)}$). Da es sich um einen kontinuierlichen Datenstrom handelt darf nicht geteilt werden, denn diese Last ist ja immer zulässig. Hier ist es sinnvoll noch 10% Sicherheitsaufschlag zu kalkulieren, da neben der reinen Datenmenge auch noch andere Informationen transportiert werden müssen. Daher wurde der errechnete Wert von 14745600 Bytes noch mit 1,1 multipliziert.

Im Folgenden werden die Variablen vorgestellt mit Default-Werten für das hier angeführte Beispiel mit dem gelegentlichen CD download für einen DSL-6000 Anschluss.

C3SURF_TRAFFIC_BYTES C3SURF_TRAFFIC_BYTES='386317473'

Wertebereich: natürliche Zahlen

Legt die Anzahl der Bytes fest, die maximal in der Zeit [C3SURF_TRAFFIC_MINUTES](#) (Seite 25) heruntergeladen werden darf. Hier als Beispiel der 1,9te Teil einer 700MB CD. Für das Beispiel mp3-Hören mit 128kBit ist hier 16220160 einzutragen.

C3SURF_TRAFFIC_MINUTES C3SURF_TRAFFIC_MINUTES='16'

Wertebereich: natürliche Zahlen

Legt die Zeit in Minuten fest, die zwischen zwei Messungen des Datenvolumens verstreicht. Wird nach der hier abgelaufenen Zeit eine Überschreitung festgestellt, so wird der Verursacher zunächst temporär gespeichert. Wird bei der nächsten Messung wieder eine Überschreitung festgestellt, so erfolgt automatisch die Abmeldung und Sperrung (für [C3SURF_TRAFFIC_BLOCKTIME](#) (Seite 25) Minuten). Wird bei der zweiten Messung keine Überschreitung mehr festgestellt, wird die temporäre Speicherung wieder gelöscht. Ist wie mit den Punkten in Flensburg, unauffälliges Verhalten führt zur Löschung von zuvor gesammelten Punkten. Wer schnell genug sammelt wird dort ja auch gesperrt.

Für das mp3-Beispiel ist hier natürlich '15' einzustellen.

C3SURF_TRAFFIC_BLOCKTIME C3SURF_TRAFFIC_BLOCKTIME='60'

Wertebereich: ganze Zahlen

Legt die Zeit in Minuten fest, die ein Zugang nach Überschreitung des Traffic-Limits gesperrt wird.

5 Allgemeines zu C3SURF

5.1 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" verfügen, aber mit FreeSurf arbeiten sollen.
Der fli4l-Admin mit dem Recht "all" sieht es sowieso und kann alles damit tun.
- Das OPT C3SURF trägt sich im Web-Admin unter "Opt" immer als "c3Surf" ein.

5.2 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
600	10080	-2	10 Stunden innerhalb einer Woche mit beliebig vielen Unterbrechungen
0	-1	0	Unendliche Zeit mit jeder Anmeldung, keine Sperre nach Ablauf der Zeit

5.3 Systemanforderungen

Wichtig: Nicht für fli4l Version 3.0.x oder frühere.

Wichtig: Der fli4l muss als DNS-Server bei den Clients eingetragen sein und muss befähigt sein Namen aufzulösen. Dazu

- benötigt er einen "Forward" auf den DNS-Server des Netzes oder
- er ist selbst der DNS-Server und kann ggf. automatisch Verbindungen aufbauen.

Sonst gibt es Probleme automatisch auf die Anmeldeseite umzuleiten. Die kann aber immer noch manuell durch die Eingabe ihrer URL aufgerufen werden.

6 Sonstiges zu C3SURF

6.1 WARNUNG

Wichtig: Ohne `"OPT_LOGINUSR='yes'"` (Seite 15) 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".

6.2 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.

6.3 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-Newsgruppen <http://www.fli4l.de/hilfe/newsgruppen/> nutzen, ich lese diese.

6.4 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.

6.5 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.

6.6 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 C3SURF 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.

Seit der Version 2.3.0 kann C3SURF auch Gutscheine generieren.

Mit der Version 2.3.1 kam eine erste rudimentäre (experimentelle) Steuerungsfunktion zur Unterbindung von übermäßigem Download-Volumen hinzu.

A.2 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:	16. September 2009	Frank und Helmut	

A.3 Andere Opt's und Howto

A.3.1 cpmvrmllog 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.3.2 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

C3SURF_BLOCK_PORT_N, 12
C3SURF_BLOCK_PORT_x, 12
C3SURF_BLOCKTIME, 9
C3SURF_CHECK_ARP, 9
C3SURF_CHECK_CURFEW, 14
C3SURF_CONTROL_HOST_OR_NET_N, 9
C3SURF_CONTROL_HOST_OR_NET_x, 10
C3SURF_CONTROL_PORT_N, 11
C3SURF_CONTROL_PORT_x, 11
C3SURF_CONTROL_SQUID, 14
C3SURF_COUNTER, 8
C3SURF_DOLOG_HTTPD, 5
C3SURF_DOLOG_INVALID, 5
C3SURF_DOLOG_LOGIN, 5
C3SURF_DOLOG_PAGE, 5
C3SURF_HTTPD_LISTENIP, 13
C3SURF_HTTPD_PORT, 13
C3SURF_LOG_PATH, 5
C3SURF_PERSISTENT_PATH, 6
C3SURF_PORTAL_DEFAULT_LANG, 14
C3SURF_PORTAL_LANGUAGES, 14
C3SURF_QUOTA, 7
C3SURF_SAVE_QUOTA, 9
C3SURF_SLOPPY_MAC, 14
C3SURF_TIME, 9
C3SURF_TRAFFIC_BLOCKTIME, 25
C3SURF_TRAFFIC_BYTES, 25
C3SURF_TRAFFIC_MINUTES, 25
C3SURF_VOUCHER_DEL_CRON, 21
C3SURF_VOUCHER_GEN_CRON, 22
C3SURF_VOUCHER_N, 20
C3SURF_VOUCHER_PRTUPDATE, 22
C3SURF_VOUCHER_PWD CAP, 23
C3SURF_VOUCHER_PWDLEN, 23
C3SURF_VOUCHER_PWDMOD, 23
C3SURF_VOUCHER_USRCAP, 22
C3SURF_VOUCHER_USRLEN, 22
C3SURF_VOUCHER_x_COUNT, 20
C3SURF_VOUCHER_x_DAYS, 20
C3SURF_VOUCHER_x_LIVES, 21
C3SURF_VOUCHER_x_TIME, 20
C3SURF_WORKON_TMP, 7
LOGINUSR_ACCOUNT_N, 15
LOGINUSR_ACCOUNT_x_BLOCKTIME, 17
LOGINUSR_ACCOUNT_x_COUNTER, 17
LOGINUSR_ACCOUNT_x_CURFEW, 18
LOGINUSR_ACCOUNT_x_EMAIL, 16
LOGINUSR_ACCOUNT_x_FORENAME, 16
LOGINUSR_ACCOUNT_x_OVERWRITE, 16
LOGINUSR_ACCOUNT_x_PWD, 16
LOGINUSR_ACCOUNT_x_SURNAME, 16
LOGINUSR_ACCOUNT_x_TIME, 17
LOGINUSR_ACCOUNT_x_USER, 16
LOGINUSR_DELETE_PERSISTENT_DATA, 15
OPT_C3SURF, 5
OPT_C3SURF_TRAFFIC, 24
OPT_C3SURF_VOUCHER, 19
OPT_LOGINUSR, 15