Paket HTTPD - Status-Webserver
Version 3.10.4

Frank Meyer
E-Mail: frank@fli4l.de

Das fli4l-Team
E-Mail: team@fli4l.de

25. Oktober 2015

Inhaltsverzeichnis

1. Dokumentation des Paketes HTTPD **3**
1.1. HTTPD - Status-Webserver . . . 3
1.1.1. OPT_HTTPD - Mini-Webserver als Statusmonitor . . . 3
1.1.2. Nutzerverwaltung . . . 4
1.1.3. OPT_OAC - Online Access Control . . . 5

A. Anhang zum Paket HTTPD **8**
A.1. HTTPD . . . 8
A.1.1. Zusätzliche Einstellungen . . . 8
A.1.2. Allgemeine Bemerkungen . . . 8

Abbildungsverzeichnis **9**

Tabellenverzeichnis **10**

Index **11**

1. Dokumentation des Paketes HTTPD

1.1. HTTPD - Status-Webserver

1.1.1. OPT_HTTPD - Mini-Webserver als Statusmonitor

Wer aus irgendeinem Grund keine Möglichkeit hat, den IMONC zu benutzen, weil er z.B. einen Mac benutzt, kann den Webserver benutzen, um den Status des fli4l-Routers abzurufen oder zu ändern. Mit `OPT_HTTPD='yes'` kann man den Statusmonitor verwenden.

Um den Status abzurufen, muss man in seinen Browser eine der folgenden Adressen eingeben:

```
http://fli4l/
http://fli4l.domain.lan/
http://192.168.6.1/
```

Hat der fli4l-Router einen abweichenden Namen, muss dieser statt "fli4l" verwendet werden. Dies gilt auch für den Domain-Namen und die obige IP-Adresse. Hat man den Webserver auf einen anderen Port gelegt (per `HTTPD_PORT`), muss man diesen mit angeben:

```
http://fli4l:81/
```

Es wird seit der Version 2.1.12 eine Login-Seite angezeigt, die nicht passwortgeschützt ist. Die passwortgeschützten Seiten befinden sich im Unterverzeichnis admin, also beispielsweise:

```
http://fli4l.domain.lan/admin/
```

Der Webserver lässt sich über folgende Variablen anpassen:

HTTPD_GUI_LANG Hiermit wird die Sprache eingestellt, in der das Webinterface dargestellt werden soll. Wird hier 'auto' eingetragen, wird die Spracheinstellung der Variablen `LOCALE` (in der base.txt) verwendet.

HTTPD_GUI_SKIN Diese Variable beeinflusst das Aussehen der Oberfläche. Das Paket *httpd_skins* stellt mit den Werten *fixed* und *notfixed* zwei alternative Darstellungen zur Verfügung. Standardwert dieser Variable ist *default*.

HTTPD_LISTENIP Der Webserver bindet sich normalerweise an eine sogenannte Wildcard-Adresse, so dass er auf einem beliebigen Interface angesprochen werden kann. Soll er sich nur an eine IP-Adresse binden, so kann es mit diesem Parameter eingestellt werden. Dazu die IP-Adressse wie folgt eintragen: `IP_NET_x_IPADDR`. Normalerweise bleibt dieser Parameter leer, damit die Standardeinstellung (ansprechbar auf einer beliebigen IP) greift.

Dieser Parameter dient lediglich dazu, den httpd nur an eine IP zu binden, so dass sich andere Instanzen an die anderen IPs des Routers binden können. Er kann nicht ohne weiteres dazu genutzt werden, den Zugang einzelner Subnetze zum Webinterface des Routers zu sperren. Dazu benötigt man weiterhin die Hilfe des Paketfilters.

Es ist auch möglich, hier durch Leerzeichen getrennt mehrere IP anzugeben.

HTTPD_PORT Soll der Webserver auf einem anderen Port laufen als 80, so ist dieser Wert anzupassen. Das ist normalerweise nicht zu empfehlen, da dann z.B. mit http://fli4l:81/ auf den Webserver zugegriffen werden muß.

HTTPD_PORTFW Setzt man diese Variable auf 'yes', kann man über das Webinterface Änderungen an der Portweiterleitung vornehmen. Es können Regeln gelöscht und hinzugefügt werden, Änderungen werden sofort wirksam. Änderungen an den Regeln gelten nur für die Laufzeit des Routers. Wird der Router neu gestartet, sind die Änderungen weg.

Diese Variable hat einen Defaultwert von 'yes'.

HTTPD_ARPING Der Webserver stellt den Online-Zustand der mit `HOST_x` aufgelisteten Hosts dar. Dazu verwendet er den *"Arp-Cache"*, ein Zwischenspeicher der die Adressen der lokalen Hosts zwischenspeichert. Hat ein Rechner lange nicht mehr mit dem Router kommuniziert, verschwindet seine Adresse aus dem *"Arp-Cache"* und der Host scheint aus zu sein. Will man den *"Arp-Cache"* aktuell halten (also das rausfallen eigentlich nicht benötigter Einträge verhindern), kann man `HTTPD_ARPING` auf *'yes'* setzen.

HTTPD_ARPING_IGNORE_N Legt die Anzahl der zu Ignorierenden Einträge fest

HTTPD_ARPING_IGNORE_x IP-Adresse oder Name des Hosts der nicht bei den ARPING-Test geprüft werden soll. Dies kann z.B. sinnvoll sein, bei Hosts die durch die regelmäßigen Netzwerpakete Ihren Akku schneller verbrauchen (Handys im WLAN).

1.1.2. Nutzerverwaltung

Der Webserver bietet eine ausgefeilte Benutzerverwaltung:

HTTPD_USER_N Hiermit wird die Anzahl der Benutzer eingestellt. Wird diese Variable auf 0 gesetzt, wird die Benutzerverwaltung komplett deaktiviert und jeder hat die Möglichkeit, auf den Webserver zuzugreifen.

HTTPD_USER_x_USERNAME HTTPD_USER_x_PASSWORD HTTPD_USER_x_RIGHTS Hier werden Benutzername und Passwort der einzelnen Benutzer eingetragen. Desweiteren wird für jeden Benutzer angegeben, auf welche Funktionen des Webservers er zugreifen darf. Diese Funktion wird mit der Variable `HTTPD_RIGHTS_x` geregelt. Im einfachsten Fall steht dort nur 'all', was bedeutet, dass der entsprechende Benutzer alles darf. Ansonsten hat die Variable den folgenden Aufbau:

```
'bereich1:recht1,recht2,... bereich2:...'
```

Statt für einen Bereich die einzelnen Rechte anzugeben, darf auch hier das Wort "all" eingesetzt werden, was wiederum heißt, das dieser Benutzer in diesem Bereich alle Rechte hat. Dabei gibt es folgende Bereiche und Rechte:

Bereich "status" Alles, was im Menü Status zu sehen ist.

view Der Benutzer darf alle Menüpunkte aufrufen.

dial Der Benutzer darf wählen und auflegen.

boot Der Benutzer darf den Router herunterfahren & neu starten.

link Der Benutzer darf Kanalbündlung an- und abschalten.

circuit Der Benutzer darf den Circuit wechseln.

dialmode Der Benutzer daf den Dialmode (Auto, Manual, Off) ändern.

conntrack Der Benutzer darf die aktuell über den Router laufenden Verbindungen ansehen.

dyndns Der Benutzer darf Log-Meldungen des DYNDNS (Seite **??**) Paketes sehen.

Bereich "logs" Alles, was mit Logdateien zu tun hat (Verbindungen, Anrufe, Syslog)

view Der Benutzer darf die Logdateien betrachten.

reset Der Benutzer darf die Logdateien löschen.

Bereich "support" Alles, was nützlich ist, wenn man beispielsweise in der Newsgroup Hilfestellung sucht.

view Der Benutzer darf die Links zur Doku, fli4l-Webseite, usw. abrufen

systeminfo Der Benutzer darf detaillierte Informationen zur Konfiguration und zum aktuellen Status des Routers (z. B.: Firewall) abfragen.

Hier noch einige Beispiele:

HTTPD_USER_1_RIGHTS='all' Diese Angabe erlaubt einem Benutzer alles!

HTTPD_USER_2_RIGHTS='status:view logs:view support:all' Dieser Benutzer darf sich zwar alles ansehen, aber nichts ändern.

HTTPD_USER_3_RIGHTS='status:view,dial,link' Dieser Benutzer darf sich den Status der Internetverbindung ansehen, wählen und Kanalbündelung ein- und ausschalten.

HTTPD_USER_4_RIGHTS='status:all' Dieser Benutzer darf alles mit der Internetverbindung machen und neu starten (natürlich auch herunterfahren). Er darf aber nicht die Logdateien sehen oder löschen, die Timetable darf er auch nicht sehen...

1.1.3. OPT_OAC - Online Access Control

OPT_OAC (optionale Variable)

Aktiviert das Modul 'Online Access Control'. Hierüber kann der Internet-Zugang jedes im Paket dns_dhcp (Seite **??**) konfigurierten Rechners selektiv deaktiviert werden.

Es gibt auch ein Kommandozeilen-Tool, welches die Steuerung über andere Pakete wie z.B. EasyCron möglich macht:

/usr/local/bin/oac.sh

Die Optionen werden beim Aufruf angezeigt.

OAC_WANDEVICE (optionale Variable)

Schränkt die Online Zugangssperre auf Verbindungen über dieses Netzwerkdevice ein. z.B. 'pppoe'

OAC_INPUT (optionale Variable)

Bietet Schutz vor der Umgehung via Proxy.

OAC_INPUT='default' sperrt die konfigurierten Ports von: Privoxy, Squid, Tor, SS5, Transproxy.

OAC_INPUT='tcp:8080 tcp:3128' sperrt TCP Port 8080 und 3128. Dies ist eine Space-separierte Liste an zu sperrenden Ports mit dazugehörendem Protokoll (udp, tcp). Fehlt das Protokoll, werden udp und tcp Ports gesperrt.

Weglassen dieser Variable oder Inhalt 'no' deaktiviert die Funktion.

OAC_ALL_INVISIBLE (optionale Variable)

Schaltet die Gesamtübersicht aus, wenn mindestens eine sichtbare Gruppe existiert. Existiert nicht mindestens eine sichtbare Gruppe, so hat diese Variable keine Wirkung.

OAC_LIMITS (optionale Variable)

Gibt eine durch Leerzeichen getrennte Liste der Zeitlimits an, die zur Auswahl stehen. Die Limits werden in Minuten angegeben. Damit kann eine zeitlich limitierte Sperre oder Freigabe erreicht werden.

Default: '30 60 90 120 180 360 540'

OAC_MODE (optionale Variable)

Mögliche Werte: `'DROP'` oder `'REJECT'` (default)

OAC_GROUP_N (optionale Variable)

Anzahl der Clientgruppen. Dient der Übersichtlichkeit, erlaubt aber auch über das Web-Interface eine gesamte Gruppe gesammelt freizugeben oder zu sperren.

OAC_GROUP_x_NAME (optionale Variable)

Name der Gruppe - Dieser Name wird im Web-Interface angezeigt und ist auch über die das Kommandozeilenscript 'oac.sh' nutzbar.

OAC_GROUP_x_BOOTBLOCK (optionale Variable)

Wenn hier 'yes' steht, werden alle Clients der Gruppe beim Bootvorgang bereits gesperrt. Hilfreich, wenn Rechner idr. gesperrt sein sollen und nur ausnahmsweise nicht.

OAC_GROUP_x_INVISIBLE (optionale Variable)

Markiert die Gruppe als unsichtbar. Sinnvoll, wenn einige Rechner vorgesperrt werden sollen aber diese nicht als eigene Gruppe im Web-If sichtbar sein sollen. Das Kommandozeilentool oac.sh kann diese trotzdem ansprechen, wenn man das braucht, z.B. von easycron aus.

OAC_GROUP_x_CLIENT_N (optionale Variable)

Anzahl der Clients in der Gruppe.

OAC_GROUP_x_CLIENT_x (optionale Variable)

Name des Clients - Siehe Paket dns_dhcp (Seite **??**).

OAC_BLOCK_UNKNOWN_IF_x (optionale Variable)

Liste der in base.txt definierten Interfaces, auf welchen nur in dns_dhcp.txt definierte Hosts ins Internet dürfen. Nicht-definierte Hosts sind hier damit generell gesperrt.

A. Anhang zum Paket HTTPD

A.1. HTTPD

A.1.1. Zusätzliche Einstellungen

Diese Einstellungen stehen normalerweise nicht in der Konfigurationsdatei, müssen also hinzugefügt werden, wenn sie benötigt werden.

HTTPD_USER Mit dieser Option ist es möglich, den Webserver mit den Rechten eines anderen Benutzers als „root" laufen zu lassen. Dies ist besonders sinnvoll, wenn der Webserver benutzt wird, um andere Seiten als das Admin-Interface bereitzustellen. Achtung: Es kann sein, dass einige Scripts, die Zugriff auf Konfigurationsdateien brauchen, dann nicht mehr laufen. Die Standard-Scripts dieses Pakets laufen unter jedem Benutzer.

A.1.2. Allgemeine Bemerkungen

Wenn man TELMOND installiert hat, werden auf der Status- und der Calls- Seite die Telefonnummern der Anrufer angezeigt. Eine Namenszuordnung lässt sich in der Datei opt/etc/phonebook vornehmen. Diese Datei hat das gleiche Format wie die Telefonnummerndatei vom IMONC. Es können also Telefonbücher zwischen IMONC und Router ausgetauscht werden. Das Format jeder Zeile ist dabei "Telefonnummer=Name[,WAV-Datei]" (ohne die Anführungszeichen). Die WAV-Datei wird aber nur vom IMONC benutzt und vom Webserver ignoriert.

Das komplette Webinterface ist seit der Version 2.1.12 auf ein Framefreies Design mit CSS umgestellt worden. Alte Browser könnten damit Probleme haben. Allerdings hat das den Vorteil, dass man das Aussehen der Oberfläche fast beliebig verändern kann, einfach indem man die CSS-Dateien (im wesentlichen /opt/srv/www/css/main.css) anpasst.

Das Webserver-Paket wurde von Thorsten Pohlmann (E-Mail: pohlmann@tetronik.com) erstellt und wird zur Zeit von Tobias Gruetzmacher (E-Mail: fli4l@portfolio16.de) gepflegt. Das neue Design (seit der Version 2.1.12) wurde von Helmut Hummel (E-Mail: hh@fli4l.de) realisiert.

Abbildungsverzeichnis

Tabellenverzeichnis

Index

HTTPD_ARPING, 4
HTTPD_ARPING_IGNORE_N, 4
HTTPD_ARPING_IGNORE_x, 4
HTTPD_GUI_LANG, 3
HTTPD_GUI_SKIN, 3
HTTPD_LISTENIP, 3
HTTPD_PORT, 3
HTTPD_PORTFW, 4
HTTPD_USER, 8
HTTPD_USER_N, 4
HTTPD_USER_x_PASSWORD, 4
HTTPD_USER_x_RIGHTS, 4
HTTPD_USER_x_USERNAME, 4

OAC_ALL_INVISIBLE, 6
OAC_BLOCK_UNKNOWN_IF_x, 6
OAC_GROUP_N, 6
OAC_GROUP_x_BOOTBLOCK, 6
OAC_GROUP_x_CLIENT_N, 6
OAC_GROUP_x_CLIENT_x, 6
OAC_GROUP_x_INVISIBLE, 6
OAC_GROUP_x_NAME, 6
OAC_INPUT, 5
OAC_LIMITS, 6
OAC_MODE, 6
OAC_WANDEVICE, 5
OPT_HTTPD, 3
OPT_OAC, 5