OpnSense HTTPS einrichten

diese PlugIns installieren:

os-acme-client
os-haproxy

ACME Client

noch **nicht** enablen

Account einrichten

- Enabled ankreuzen
- beliebigen Name und Beschreibung vergeben
- ACMA CA: Let's encrypt auswählen

Challenge Type einrichten

- Enabled ankreuzen
- Name und Beschreibung: Validation:via_HTTP-01
- Challenge Type: HTTP-01
- HTTP Service: HAProxy HTTP Frontend... (das geht evt erst später, wenn HAproxy fertig eingerichtet ist, dann hier nicht vergessen !)

Automation

- Enabled ankreuzen
- Name und Beschreibung: RestartHAProxy
- Run Command: Restart HAProxy (OPNsense Plugin)

Certificates

- Enabled ankreuzen
- Common Name: Name der Hauptseite, z.B.: www.dj0abr.de
- Beschreibung: dj0abr_certificate
- Alt Names: alle weiteren URLs wie z.B.: wx.dj0abr.de usw.
- ACME Account: oben angelegter Account
- Challenge Type: oben angelegter: Validation:via_HTTP-01
- Auto Renewal ankreuzen und Interval zB 60 eingeben
- Key Length: 4096
- Automations: RestartHAProxy (wurde vorhin eingerichtet)
- Not using DNS alias mode

Settings

- Enable, Auto Renewal, HAProxy Integration ankreuzen

Konfiguration testen und Apply.

zurück zum Menü: Certificates und Issue/Renew drücken

In LogFiles prüfen ob es erfolgreich läuft.

HAProxy

Settings - Real Server

hier werden die tatsächlich vorhandenen Webserver eingetragen, alles natürlich Port 80 (weil 443 ja OPNsense selbst macht). Das sind z.B.: dj0abr_de_80, ein statischer Webserver auf seiner IP und Port 80. Mode: active. Alles andere (SSL) ausgeschaltet oder default lassen.

Das gleich für die weiteren Webserver wie zB wx_dj0abr_de_80 machen.

Backend

Als nächstes einen Backend Pool für jeden Webserver anlegen:
z.B.: Name und Beschreibung: pool_dj0abr_de_80 mit Mode HTTP(Layer7)und Source-IP-Hash.

Bei Servers: den entsprechenden Server auswählen, und Advertise Protocols (ALPN): HTTP/2 und HTTP/1.1
Table Type: Source-IP (ist sowieso default so wie auch alles andere)

Rules/Checks: Condition

für jede URL eine Condition anlegen, also für
www.dj0abr.de und auch für
dj0abr.de

damit ist es egal ob der User www mit angibt oder nicht

Cond.Type: Host matches
Host String: www.dj0abr.de und in einer anderen Condition dj0abr.de und auch wx.dj0abr.de usw. was man braucht

Rules/Checks: Rules

hier wird festgelegt was passieren soll wenn eine Condition passt, es muss also für jeden Webserver eine Rule angelegt werden, z.B.:

- Name und Beschreibung: rule_www_dj0abr_de_80
- Test Type: IF
- hier alle Conditions auswählen, die zu dem entsprechenden Webserver passen
- Logical Operator: OR
- Execute: Use spec. Backend Pool
- Use backend pool: den Pool des gewünschten Webservers angeben

hier habe ich noch eine spezielle Rule (möglicherweise kann man das erst eintragen, wenn alles andere fertig ist):

- Name und Beschreibung: HTTPredirect
- Test Type: IF
- Select Conditions: no_acme_challenge. SSLestablished
- Logical Op: AND
- Exec: http-request redirect
- HTTP redirect: scheme https code 301

Virtual Services: Public Frontend

hier der Einstieg für HTTPS (Port 443):

- Name und Beschreibung: pub_dj0abr_de_443
- Listen Address: 0.0.0.0:443 * *Type: HTTP/HTTPS (SSL offloading)*
- Default Backend Pool: none * *Enable SSL offloading ankreuzen*
- Certificates: das oben erstelle Cert. auswählen * *min SSL: TLSv1.2*
- max SSL: None * *Cipher List: ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256*
- Cipher Suites: TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256 * *Enable HSTS ankreuzen*
- HSTS max-age: 15768000 * *Advertise Prot: HTTP/2 und HTTP/1.1*
- Select Rules: alle Rules auswählen die zu dem Webserver gehören, also: rule_www_dj0abr_de_80 und rule_wx_dj0abr_de_80 *und hier noch der Einstieg für Port 80: * Name und Beschreibung: pub_dj0abr_de_80*
  * *Listen Address: 0.0.0.0:80*
- Type: HTTP/HTTPS (SSL offloading) * *Default Backend Pool: none*
- Enable SSL offloading **NICHT** ankreuzen * *Advertise Prot: HTTP/2 und HTTP/1.1*
- Select Rules: redirect_acme_challenges und HTTPredirect

Firewall: Ports freigeben

In den Rules für das WAN Interface:

Damit Port 80 zum HTTP Proxy durchkommt:

Pass WAN Interface (in, IP4, TCP) zu Destination: This Firewall from/to: HTTP

und das gleiche nochmal für Port 443.