Tvheadend - Feature #5489

Add opportunistic TLS (STARTTLS) to HTSP

2019-01-10 06:55 - Dietmar Konermann

Status:	New	**Start date:**	2019-01-10
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Just to have this officially requested and tracked... :)
IMHO, sooner or later it's desireable for a grown-up protocol like HTSP to offer encryption, e.g. by opportunistic TLS (STARTTLS).

Cheers,
Dietmar

History

#1 - 2019-05-15 23:09 - Flole Systems

Let's actually get this going:

I've looked into it a little and it seems a lot easier than expected. Basically we have to call the following when starttls command is sent:

```
ssl = SSL_new(ctx);
        SSL_set_fd(ssl, client);

        if (SSL_accept(ssl) <= 0) {
            ERR_print_errors_fp(stderr);
        }
        else {
            SSL_write(ssl, reply, strlen(reply));
        }
```

That code was taken from https://wiki.openssl.org/index.php/Simple_TLS_Server

When reading or writing all we have to do is check if ssl != Null and then use the ssl_read or ssl_write. The only thing that could cause issues is that writing is currently a special method which writes each byte individually, not sure what would happen if we replace that call with a single ssl_write.

Any thoughts on this? Maybe someone knows why that tvh_write was necessary? Ideas for improvements? Suggestions?

Also this should be made optional by something like #ENABLE_SSL so there can be builds without SSL.